FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 69
Page 241 ~ b6 - -1,5; b7C - -1,5; b7E - -1,9;
Page 242 ~ b6 - -1,5; b7C - -1,5; b7E - -1,9;
Page 243 ~ b6 - -5; b7C - -5; b7E - -1,9;
Page 244 ~ b6 - -1,5; b7C - -1,5; b7E - -1,9;
Page 293 ~ Duplicate;
Page 319 ~ b6 - -1; b7C - -1; b7E - -6;
Page 320 ~ b7E - -6;
Page 413 ~ Duplicate - to Section 4;
Page 414 ~ Duplicate - to Section 4;
Page 415 ~ Duplicate - to Section 4;
Page 416 ~ Duplicate - to Section 4;
Page 417 ~ Duplicate - to Section 4;
Page 418 ~ Duplicate - to Section 4;
Page 419 ~ Duplicate - to Section 4;
Page 420 ~ Duplicate - to Section 4;
Page 421 ~ Duplicate - to Section 4;
Page 422 ~ Duplicate - to Section 4;
Page 423 ~ Duplicate - to Section 4;
Page 424 ~ Duplicate - to Section 4;
Page 425 ~ Duplicate - to Section 4;
Page 426 ~ Duplicate - to Section 4;
Page 427 ~ Duplicate - to Section 4;
Page 428 ~ Duplicate - to Section 4;
Page 429 ~ Duplicate - to Section 4;
Page 430 ~ Duplicate - to Section 4;
Page 431 ~ Duplicate - to Section 4;
Page 432 ~ Duplicate - to Section 4;
Page 433 ~ Duplicate - to Section 4;
Page 434 ~ Duplicate - to Section 4;
Page 435 ~ Duplicate - to Section 4;
Page 436 ~ Duplicate - to Section 4;
Page 437 ~ Duplicate - to Section 4;
Page 438 ~ Duplicate - to Section 4;
Page 439 ~ Duplicate - to Section 4;
Page 440 ~ Duplicate - to Section 4;
Page 441 ~ Duplicate - to Section 4;
Page 442 ~ Duplicate - to Section 4;
Page 443 ~ Duplicate - to Section 4;
Page 444 ~ Duplicate - to Section 4;
Page 445 ~ Duplicate - to Section 4;
Page 446 ~ Duplicate - to Section 4;
Page 447 ~ Duplicate - to Section 4;
Page 448 ~ Duplicate - to Section 4;
Page 449 ~ Duplicate - to Section 4;
Page 450 ~ Duplicate - to Section 4;
Page 451 ~ Duplicate - to Section 4;
Page 452 ~ Duplicate - to Section 4;
Page 453 ~ Duplicate - to Section 4;

```
XXXXXXXXXXXXXXXXXXXXXXXXX
X    Deleted Page(s)      X
X    No Duplication Fee X
X    For this Page       X
XXXXXXXXXXXXXXXXXXXXXXXXX
```

b6 -1,2
b7C -1,2

02/26/2002 08:11 PM

To:
cc:

Subject: NYT Hacker Article just posted --

http://online.securityfocus.com/news/342NEWS
   New York Times Internal Network Hacked

   How open proxies and default passwords led to Adrian Lamo padding his rolodex with information on 3,000
   op-ed writers, from William F. Buckley Jr. to Jimmy Carter.

   By Kevin Poulsen
   Feb 26 2002 4:15PM PT

   Security holes in the New York Times internal network left sensitive databases exposed to hackers, including a file
   containing social security numbers and home phone numbers for contributors to the Times op-ed page, SecurityFocus
   Online has learned.

   In a two-minute scan performed on a whim, twenty-one-year-old hacker and sometimes-security consultant Adrian Lamo
   discovered no less than seven misconfigured proxy servers acting as doorways between the public Internet and the
   Times' private intranet, making the latter accessible to anyone capable of properly configuring their Web browser.

   "The very first server I looked at was running an open proxy," says Lamo. "The server practically approached me."

   Once on the newspaper's network, Lamo exploited weaknesses in the Times password policies to broaden his access, eventually browsing such disparate information as the names and social security numbers of the paper's employees, logs of home delivery customers' stop and start orders, instructions and computer dial-ups for stringers to file stories, lists of contacts used by the Metro and Business desks, and the "WireWatch" keywords particular reporters had selected for monitoring wire services.

   But measured by sheer star power, the hack is most notable for Lamo's access to a database of 3,000 contributors to the Times op-ed page, the august soap box of the cultural elite and politically powerful.

   The roster includes social security numbers for former U.N. weapons inspector Richard Butler, Democratic operative
   James Carville, ex-NSA chief Bobby Inman, Nannygate veteran Zoe Baird, former secretary of state James Baker,

FBI(19-cv-1495)-1607

Internet policy thinker Larry Lessig, and thespian activist Robert Redford, who last May authored an op-ed on President
Bush's environmental policies.

Entries with home telephone numbers include Lawrence Walsh, William F. Buckley Jr., Jeanne Kirkpatrick, Rush
Limbaugh, Vint Cerf, Warren Beatty and former president Jimmy Carter.

The database includes details on contributors' areas of expertise and what books they've written, and the odd note on
how easily they succumb to editing or how much they were paid.

Lamo notified the Times of the vulnerabilities Tuesday through a reporter, and provided them with a list of the open
proxies. In a statement, a spokesperson for the paper said the Times takes security "very seriously."

"We are actively investigating a potential security breach," wrote Times spokesperson Christine Mohan. "Based on the
results of this investigation we will take appropriate steps to ensure the security of our network."

Hacker's Helpful History
Adrian Lamo has built an unusual reputation exposing security holes at large corporations, then voluntarily helping them
fix the vulnerabilities he exploited -- sometimes visiting their offices or signing non-disclosure agreements in the process.

In December, Lamo was praised by communications giant WorldCom after he discovered, then helped close, security
holes in their intranet that threatened to expose the private networks of Bank of America, CitiCorp, JP Morgan, and
others.

In September, the hacker used a vulnerable Web-based production tool to tamper with a wire service story on Yahoo!
News, deliberately choosing an old story to minimize the impact.

The hacker professes relief at discovering that the Times intranet afforded him no similar opportunity to modify stories in
the paper's print edition, without clearing human hurdles in the Times editorial process. "It's really better for everybody if
the New York Times has the ability to runs something unusually every now and then without people checking it for my
writing style," says Lamo.

The newspaper's public Web site -- the target of a high-profile defacement in 1998 -- is outsourced, and wasn't affected
by the vulnerabilities.

Privacy Concerns
Lamo says he began his excursion at a proxy in the Times home delivery department and scanned the newspaper's IP
address range for Web servers. "The proxy was on a different network, dealing with

2

management of subscription

information, but it was trusted by their internal network," says Lamo. He quickly found the intranet homepage, and an

unprotected copy of a database that cataloged employees' names and social security numbers. "From what I've been

able to tell, it was a backup database being used for research."

Armed with that information, the hacker could use the intranet account of any employee that hadn't changed their

password from the default -- the last four digits of the person's social security number. One of those belonged to a

worker that had the power to create new accounts, so Lamo set up his own account on the network with higher

privileges.

From there, it was a short hop to the op-ed database.

"This is sort of a situation where security and privacy intersect," says David Sobel, an attorney with the Electronic

Privacy Information Center (EPIC). "One of the concerns with the online availability of personal information is the lack of

security that often surrounds those kinds of systems... There's an ethical obligation to protect this data, given the harm

that can result in the form of identity theft from obtaining a social security number."

This isn't the first time personal information on the rich and powerful has been compromised by weak network security.

One year ago, anti-globalization hackers penetrated a database maintained by the World Economic Forum, and

downloaded similar data on attendees of the group's summit on global economic trends in Davos, Switzerland, including

Bill Gates, Bill Clinton, South African President Thabo Mbeki and Japanese Prime Minister Yoshiro Mori.

But with the Times hack Lamo may have gone one better. Rather than merely crossing the information wake left by the

elite, Lamo says he actually joined their ranks, creating his own entry in the 'L' section of the Times database, complete

with his real name, cell phone number, and email address.

In the space set aside for a description of the contributor's expertise, Lamo wrote, "Computer hacking, national security,

communications intelligence."

b6 -1,2
b7C -1,2

02/27/2002 10:56 AM

To:

cc:

Subject: Hacker said he did this 10 days ago

Adrian Lamo (or Lam-o for short) told an AP reporter that he hacked our intranet 10 days ago...

and FYI: Adrian called the NYC bureau of AP last nite. They couldn't reach us to confirm (?) so they didn't file a story. Sounds like he's doing a bit of PR himself...

b6 -1,2
b7C -1,2

03/04/2002 10:12 AM

To:
cc:

Subject: chats on Security Focus article

New York Times Internal Network Hacked
    by Toybreaker
    Feb 27 2002 11:25PM

    Lamo, nice work and way to keep everything on the up and up. Not many Hackers seem to have his ethics. I
    am curious if he is given any $$ for exposing these holes to the companies and not telling the world before
    fixes can be made. **If I was head of of NYT I would be more than willing to cut him a fat check for his efforts.**
    He has my respect =^}

New York Times Internal Network Hacked
    by Anonymous
    Feb 28 2002 5:42AM

    What is this?? What is the story here? A network gets "hacked" or more accurately broken into by an
    attacker that uses a misconfigured proxy. Suprise, suprise internal corporate network security is not exactly
    what it should be. Stop the presses, we got the scoop of the century! A network with poor user passwords!

    Script kiddie does not put his tag on the web site but media gives him the much wanted attention for being an
    "ethical hacker" **Many defacement groups also offer their help to the sysadmin, do you also consider them to**
    be heroic whitehat security experts ? I did not think so... **The only thing "hacked" here is the media.**

    Who wrote the story? John Markoff ?

New York Times Internal Network Hacked
    by Anonymous
    Feb 28 2002 7:41AM

    Just a brief comment.

    "Lamo notified the Times of the vulnerabilities Tuesday through a reporter, and provided them with a list of
    the open proxies."

    Why does this humble servant of all that is good and super whitehat; hacker involve a reporter before talking to the NY Times? Is he seeking attention? Does he want to have his name

b6 -1,2
b7C -1,2

03/08/2002 12:19 PM

To:

cc:

Subject: Tech TV press query -- they heard rumor we are prosecuting Lamo

The reporter said they had heard a rumor that we were moving forward with prosecuting Lamo.

I gave our standard statement that we were investigating all our options to determine what our next steps would be. That we hadn't finalized that decision yet.

Tech TV is a (shrinking) cable TV outlet, based in San Fran, that covers tech news...shouldn't be much pickup but you never know.

Looks like it will be part of tonight's show - below is the description on their site. I called to ask them to correct the reference to the NYT Web site (should by NYT Company's intranet site) and let her know that it was not information about subscribers that was allegedly accessed. She is going to change that reference to Op-Ed columnists per earlier reports/coverage.

Friday on 'Tech Live'
March 7, 2002
Homeless Hacker

The infamous homeless hacker, Adrian Lamo recently hacked into the New York Times website and snagged private information on some big-time subscribers. While the Times is considering pressing charges, he says he is hacking to warn companies about security holes. Is what Adrian is doing illegal?

P.S. They are sending me a videotape of this show.

FBI(19-cv-1495)-1612

b6 -1,2,5
b7C -1,2,5

03/25/2002 03:09 PM

To:

cc:

Subject: [_____] called to get hacker update

hacking the NYT intranet.

He asked for an update, wanted to know if we would be reporting the hacker incident as a crime to the FBI.

I said that we were still investigating all the options to determine what our next steps would be, and confirmed that yes, reporting it to the FBI was one of the options.

I'll track for his article.

Sign In | My Account | About Us | Advertise | Go

○ SecurityFocus™
O N L I N E

PERIMETER WATCH

Home | SFOnline | The Basics | Microsoft | Unix | IDS | Incidents | Virus

Search

SFOnline

b6 -1
b7C -1

Bugtraq | Mailing Lists | Library

◇ NEWS

New York Times Internal Network Hacked

How open proxies and default passwords led to Adrian Lamo padding his rolodex with information on 3,000 op-ed writers, from William F. Buckley Jr. to Jimmy Carter.
By *Kevin Poulsen*
Feb 26 1980 4:15PM PT

Security holes in the *New York Times* internal network left sensitive databases exposed to hackers, including a file containing Social Security numbers and home phone numbers for contributors to the *Times* op-ed page, SecurityFocus Online has learned.

In a two-minute scan performed on a whim, twenty-one-year-old hacker and sometimes-security consultant Adrian Lamo discovered no less than seven misconfigured proxy servers acting as doorways between the public Internet and the *Times*' private intranet, making the latter accessible to anyone capable of properly configuring their Web browser.

"The very first server I looked at was running an open proxy," says Lamo. "The server practically approached me."

Once on the newspaper's network, Lamo exploited weaknesses in the *Times* password policies to broaden his access, eventually browsing such disparate information as the names and Social Security numbers of the paper's employees, logs of home delivery

Adrian Lamo does most of his hacking with an ordinary Web browser.

customers' stop and start orders, instructions and computer dial-ups for stringers to file stories, lists of contacts used by the Metro and Business desks, and the "WireWatch" keywords particular reporters had selected for monitoring wire services.

But measured by sheer star power, the hack is most notable for Lamo's access to a database of 3,000 contributors to the *Times* op-ed page, the august soap box of the cultural elite and politically powerful.

The roster includes Social Security numbers for former U.N. weapons inspector Richard Butler, Democratic operative James Carville, ex-NSA chief Bobby Inman, Nannygate veteran Zoe Baird, former secretary of state James Baker, Internet policy thinker Larry Lessig, and thespian activist Robert Redford, who last May authored an op-ed on President Bush's environmental policies.

Entries with home telephone numbers include Lawrence Walsh, William F.

NEWS

New York Times Internal Network Hacked
Feb 26

Software That Asks 'Who Goes There?'
Feb 26

MP3 Files Not Always Safe
Feb 25

FAA: Air Traffic Control Holes Plugged
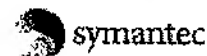Feb 21

[more . . .]

COMMENTARY

GREENE: MS to force IT-security censorship
Nov 02

LEVY: Security in an Open Electronic Society
Oct 21

LEVY: The Blind Leading the Blind
Aug 30

LEVY: Full Disclosure is a necessary evil

of the concerns with the online availability of personal information is the lack of security that often surrounds those kinds of systems... There's an ethical obligation to protect this data, given the harm that can result in the form of identity theft from obtaining a Social Security number."

This isn't the first time personal information on the rich and powerful has been compromised by weak network security. One year ago, anti-globalization hackers penetrated a database maintained by the World Economic Forum, and downloaded similar data on attendees of the group's summit on global economic trends in Davos, Switzerland, including Bill Gates, Bill Clinton, South African President Thabo Mbeki and Japanese Prime Minister Yoshiro Mori.

But with the *Times* hack Lamo may have gone one better. Rather than merely crossing the information wake left by the elite, Lamo says he actually joined their ranks, creating his own entry in the 'L' section of the *Times* database, complete with his real name, cell phone number, and email address.

In the space set aside for a description of the contributor's expertise, Lamo wrote, "Computer hacking, national security, communications intelligence."

<tips@securityfocus.com>

Discussion

[Post a comment]

FBI(19-cv-1495)-1615
2/27/02

Lamo gained access to the network using Web proxies located on the network. Proxies are machines that allows users to route through - or into - networks, often skirting past firewalls. The whole process from search to discovery took less than two minutes.

"It struck me as being a part of their network more likely to be placed in a trusted location," he said. "Ironically, it wasn't until I mistyped a URL that I found what I was looking for - the error message invited me to 'try the main New York Times intranet site' instead."

The Times' corporate intranet also allows users to access other sensitive areas, including the company's human resources department, as well as tools used to submit advertisements that accompany stories in the daily paper and the New York Times Web site, http://www.nytimes.com .

The discovery highlights just how susceptible the Internet can be as a tool for spreading misinformation. Lamo said had he been so inclined, he probably would have been able to figure out how to successfully submit a small news item or advertisement for publication.

Days after the Sept. 11 attacks, Lamo used a proxy on the Yahoo network to add satirical comment to a story on the company's Web site about Russian programmer Dmitry Sklyarov, a stunt that raised public concern about the integrity of online media.

Last week, Lamo alerted SBC Communications that several of its Web pages containing tens of thousands of subscriber user names and passwords were exposed to the Web and completely unprotected.

In December, Lamo discovered an Internet-accessible Web tool that provided easy access to the keys to private network routers for dozens of companies, including AOL Time Warner, Bank of America, Citicorp, Fox News Corp., JP Morgan, McDonalds, and Sun Microsystems - to name just a few.

When asked why he does what he does, Lamo is noncommittal and somewhat cagey, downplaying his penchant for seeing things in ways that often go unnoticed by most.

That didn't stop him, however, from quietly adding his name to the newsroom's source list as an expert on computer hacking.

"I'm not trying to bring about any sort of specific change anywhere by what I do - but in doing what I do, acting in good faith doesn't seem like a bad thing, and hoping that someone in a similar situation in some undefined future might have options that aren't all a downwards spiral doesn't seem unreasonable either," Lamo said. "It would be nice."

Reported by Newsbytes.com, http://www.newsbytes.com

19:52 CST
Reposted 08:23 CST

(20020227/WIRES ONLINE, LEGAL, BUSINESS, TELECOM/NYTIMES/PHOTO)

FBI(19 cv 1495) 1616

1 = significant mention of NYTCO
2 = passing mention of NYTCO
3 = industry article

+ = positive
- = negative
N = neutral

MSNBC HOME

Technology
HACKS, ATTACKS & SCAMS

N.Y. Times source database hacked

Paper's rich-and-famous op-ed, source database revealed

By Bob Sullivan
MSNBC

Feb. 27 — A computer security researcher accessed internal New York Times computer networks this week through the Internet and managed to view hundreds of sensitive Times files. Among them: a database of 3,000 Times op-ed page contributors. The file contained Social Security numbers and other personal information belonging to luminaries like James Carville, James Baker, Larry Lessig, and Robert Redford. The researcher also got phone numbers for William F. Buckley Jr., Rush Limbaugh, Warren Beatty and Jimmy Carter. In a statement , the New York Times said it is investigating the problem.
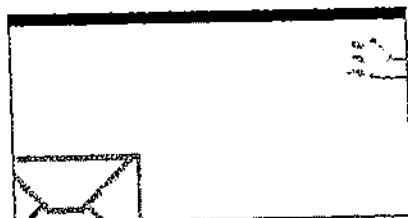
E-MAIL THIS   COMPLETE STORY

Updated every hour

information belonging to Times' employees and customers.

"This surely wasn't anything the people involved had counted on when they'd been filling out that tell-us-about-yourself account form," he said.

Lamo, a 21-year-old nomad who is among the few computer researchers that use their real name when informing a company about a security problem, said he generally does his work to improve the state of computer security at large companies. His unconventional tactics are frequently criticized, he says.

"I recognize that some people will see my actions as illegal, immoral, or worse. It's not for me to contest them or try to win them over to the Adrian Lamo School of Security," he said. "I've done my best to act in good faith and avoid harm to the company and employees involved."

TECHNOLOGY TOP STORIES

[STORY] WashPost: Foreign workers in demand
[STORY] Having your own cake and eating it
[STORY] Britney gets cyber make over
[STORY] Human chip implants stir up a debate
[STORY] Drug trafficking's Internet connection

TOP BUSINESS NEWS

[STORY] Stocks surge
[STORY] Greenspan predicts subdued recovery
[STORY] Durable-goods orders soar
[STORY] Data confirms Germany's recession
[STORY] Two key Enron figures offer cooperation for immunity

MSNBC VIEWERS' TOP 10

Would you recommend this story to other viewers?

not at all 1 - 2 - 3 - 4 - 5 - 6 - 7 highly

© BACK TO TOP ↑

MSNBC is optimized for
• Microsoft Internet Explorer
• Windows Media Player

• MSNBC Terms, Conditions and Privacy © 2002

REUTERS ⊕ .COM

New York Times internal Web site hacked

Last Updated: February 27, 2002 11:44 AM ET

🖨 Print This Article

NEW YORK, Feb 27 (Reuters) - New York Times Co. NYT.N said on Wednesday it was investigating a security breach of its internal corporate Web site, but said that security flaw has been fixed.

The company was notified on Tuesday about the breach of its internal Web site, which includes company presentations by management, internal memos and other company information, spokeswoman Christine Mohan told Reuters.

"We identified the security flaw and addressed it, and are continuing to investigate the situation to ensure the security of our network," she said.

The company was still looking into who committed the breach, how it occurred and what information was accessed, she added.

www.reuters.com

REUTERS ⊕

AtNewYork

Back to http://www.atnewyork.com/news/article/0,,8471_982161,00.html

NY Times Internal Network Hacked

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE ░░░░░░ [ ] ░░ ░░░ ░ IS

b6   1
b7C   1

By Ryan Naraine

The New York Times on Wednesday confirmed a computer hacker broke into its internal network, accessing files and folders containing personal information of some of its biggest op-ed contributors.

Acting on a whim, 21-year-old California hacker Adrian Lamo found seven misconfigured proxy servers that served as doorways between the Internet and the company's private intranet.

Once he got in, Lamo breached weaknesses in the password policies of the New York Times to expand his access to a database of op-ed contributors, which included social security numbers of people like former U.N weapons inspector Richard Butler, former Clinton aide James Carville, radio personality Rush Limbaugh, Microsoft kingpin Bill Gates, and New York City mayor Mike Bloomberg.

New York Times spokeswoman Christine Mohan confirmed the breach and said an active investigation was underway. "The New York Times Company takes the security of its network very seriously...We will take appropriate steps if necessary to ensure the security of our network," she told atNewYork.

Mohan said the company had not contacted Lamo or had not yet identified the source of the intrusion although it is widely known that the hacker immediately contacted the media company with the help of a journalist from SecurityFocus Online Web site, which first reported the story.

It is the second time the Times has been the target of hackers. In 1998, a group known as "Hacking for Girlies" (HFG) defaced the company's flagship NYTimes.com site with profanities and racial rants which targeted reporter John Markoff, who authored "TakeDown," a book on the search for convicted hacker Kevin Mitnick.

Although the latest breach happened behind the scenes, it highlights the potential security nightmares facing companies that do business on the Internet.

Lamo, who gained notoriety last year after breaching the systems of Yahoo!, Microsoft ISP WorldCom, said he was surprised at the ease in which he got access into the Times' database.

NYPOST.COM

PAGE SIX

By RICHARD JOHNSON with PAULA FROELICH and CHRIS WILSON

February 28, 2002 -- **All the news that's fit to hack**

INTIMATE information about celebrity contributors to the New York Times op-ed page was exposed after a 21-year-old hacker broke into the paper's computer system.

It only took two minutes for security consultant **Adrian Lamo** to infiltrate the Times' internal network and get private poop on the likes of **Robert Redford, Warren Beatty, Jimmy Carter, William F. Buckley Jr., Rush Limbaugh, James Carville, James Baker** and **Jeanne Kirkpatrick.**

Lamo accessed a database of 3,000 contributors to the Times' opinion page that listed social security numbers, home telephone numbers, notes about how they feel about being edited, and how much they get paid.

He also accessed the names and social security numbers of all Times employees, lists of contacts used by the metro and business desks and logs of home delivery customers' start-and-stop orders.

"The server practically approached me," Lamo bragged to SecurityFocus.com. The crafty computer whiz discovered seven servers acting as doorways between the public Internet and the Times' private intranet, making the information available to anyone capable of properly configuring a Web browser.

Lamo notified the Times of its porous database on Tuesday. In a statement, a red-faced Times spokesperson said: "We are actively investigating a potential security breach. Based on the results of this investigation we will take appropriate steps to ensure the security of our network."

Lamo has earned a reputation for hacking into the networks of large corporations, alerting the companies and offering to fix their vulnerabilities - for a price.

In December, he was praised by communications monolith WorldCom after he discovered - and helped fix - gaping holes in its intranet that threatened to expose the private networks of Bank of America, Citicorp and J.P. Morgan.

A few months earlier, he had shown how easy it was to hack into a Yahoo! News Web site by tampering with a wire service story posted on the site. At least Lamo was unable to tinker with Times stories before they got into print. The paper's Web site is not tied in to its Swiss cheese-like internal computer system.

Last year, anti-globalization activists hacked into a World Economic Forum database and downloaded details about **Bill Clinton, Bill Gates,** South African President **Thabo Mbeki** and Japanese Prime Minister **Yoshiro Moki,** all attendees of the group's summit in Davos, Switzerland.

~~Steve's gains~~

Advertising
ComPile Agency
Directory

Sections

PAGE ONE
NATION | WORLD
CITY | REGION
BUSINESS
SPORTS
LIVING | ARTS
EDITORIALS | OP-ED

Weekly
Health | Science (Tue.)
Food (Wed.)
Calendar (Thu.)
Life at Home (Thu.)

Sunday
Automotive
Focus
Learning
Real Estate
Travel

Local news
City Weekly
Globe South
Globe West
North Weekly
NorthWest Weekly
New Hampshire

Features
Globe archives
Book Reviews
Book Swap
Columns
Comics
Crossword
Horoscopes
Death Notices
Lottery
Movie Reviews
Music Reviews
NetWatch weblog
Obituaries
Special Reports
Today's stories A-Z
TV & Radio
Weather

Classifieds
Autos
BostonWorks
Real Estate
Place an Ad

The New York Times Co. owns the Times and The Boston Globe.

This story ran on page C4 of the Boston Globe on Thursday, February 28, 2002.
© Copyright 2002 Globe Newspaper Company.

[Send this story to a friend | Easy-print version | Search archives]

b6   1
b7C   1

New York Times Hack Exposes High-Profile Data

Jay Lyman

February 28, 2002

The New York Times repeatedly has been the target of computer security exploits, including a 1998 breach that resulted in defacement of its Web site.

The New York Times has confirmed that its corporate intranet -- which reportedly contains personal data on such high-profile op-ed contributors as former president Jimmy Carter, activist actors Warren Beatty and Robert Redford, and Internet gurus Vint Cerf and Larry Lessig -- was hacked earlier this week.

The breach, achieved by a well-known benevolent hacker named Adrian Lamo, reportedly came via ill-configured proxy servers that led from the Internet to the Times' intranet. That intranet includes the names and social security numbers of the company's employees, logs of home delivery orders, instructions for Times reporters and contact lists, among other sensitive data.

The Times said it has closed the security gaps and is investigating the breach, which is the latest of many exploits undertaken against the media giant.

Hacker Heads-Up

New York Times spokesperson Christine Mohan told NewsFactor that the company was notified Tuesday that there might be a security breach of its corporate intranet.

"We did confirm that there had been one," she said. "We did identify the security flaws, and then we did secure them."

Mohan said the paper received a call from network security firm SecurityFocus, which had been contacted by Lamo, alerting the Times to the security breach.

Assessing Next Steps

Mohan said the Times is not currently focused on the source of the security breach. She would not comment about whether the company is grateful that it was Lamo who hacked its internal network rather than a less benevolent hacker.

"Right now, we are focused on the situation at hand and on securing the information network," Mohan said. "We really aren't focused now on confirming the identity of this person.

2/28/02
FBI(19 cv 1495) 1623

CNET tech sites: Price Comparisons | Pro

c|net NEWS.COM
TECH NEWS FIRST

Front Page | Enterprise | E-Business | Communications | Media | Personal Technology | Investor

Who's Who in E-Business
BUSINESS — NEW AND IMPROVED WITH FLASH

Search

[News.com] [Go!]

Hacker penetrates N.Y. Times' network

By Robert Lemos and Margaret Kane
Staff Writers, CNET News.com
February 27, 2002, 12:30 PM PT

update Adrian Lamo--the curious hacker who has hit such high-profile companies as Yahoo, Microsoft and Excite@Home--has struck again, this time gaining access to *The New York Times'* internal operations network.

In an e-mail interview Wednesday with CNET News.com, Lamo described the attack, saying he viewed employee records--including Social Security numbers--and accessed the contact information for the paper's sources and columnists, including such well-known contributors as former U.S. President Jimmy Carter, former Marine Col. Oliver North and hip-hop artist Queen Latifah.

Lamo even added himself as a contact as a "computer hacking, national security and communications intelligence" specialist.

"This raises some questions about their handling of the data the company receives," Lamo said. "But in terms of the overall impact on the *Times,* it's an order of magnitude less than it could have been if people had been able to alter content" on the newspaper's public Web site, NYTimes.com.

On Wednesday, the publishing giant confirmed that the security of the internal network of its flagship newspaper had been breached. New York Times Co. spokeswoman Christine Mohan said the newspaper had addressed the security flaws, though it is still trying to determine what information was accessed and when the intrusion took place.

The security breach is the latest by Lamo, whose hack-and-tell exploits include breaking into WorldCom in December, Microsoft in October, Yahoo in September and Excite@Home in May.

Although Lamo's activities are well known, his intrusions have not resulted in any charges being filed against him. In every case, he has convinced targets that his intentions are good, notifying companies of breaches before going public. His targets have not necessarily welcomed the bad news, but his actions have allowed them to bolster their security.

The New York Times Co. would not say whether it is considering prosecuting Lamo. "Right now, we are focusing on investigating the situation," said Mohan. "We are determining what

Latest Headlines
display on desktop

Microsoft, DOJ tweak settlement terms

Chip-equip sales languish in 2001

Chinese firm to peddle IBM disk drives

Microsoft curries favor with undergrads

Senate group to consider copy controls

Will techs gain from auditor scrutiny?

Scripting flaw leaves sites vulnerable

Intel forum: Pentium 4, cheaper chips

Don't expect a low-voltage Pentium 4

Gateway's slow new year improving

Cisco shares dip on analyst forecast

U.S. government rebuilds Net image

Juniper: No losses to Cisco

Morpheus looks to Gnutella for help

Caldera reports loss, reverse stock split

House bill gives broadband boost to Bells

Dialing delirium at the Olympics

Can this man revive CMGI?

Auction placement irks eBay sellers

Compaq to sell Scotland plant

This week's headlines

Monday: Office

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED

be 1
b/C 1

INFORMATIONWEEK.COM

Hacker Adds *New York Times* To Long List Of Targets

A 21-year-old hacker gains access to the newspaper's corporate intranet and its source database. It's the latest in a long list of companies whose security problems have been exposed by hacker Adrian Lamo.

By George V. Hulme, InformationWeek
Feb 27, 2002 (12:00 AM)
URL: http://www.informationweek.com/story/IWK20020227S0003

Adrian Lamo, a homeless 21-year-old literary buff who likes to quote Ayn Rand and H.P. Lovecraft, uses an old Toshiba notebook to expose security weaknesses at companies such as Microsoft, Yahoo, AOL, and Excite@Home. He won't explain why he does what he does, but he says hacking is his nature.

In December, the part-time security and communications consultant struck WorldCom and gained access to information about the communication company's clients, including AOL Time Warner, Bank of America, Citicorp, News Corp., J.P. Morgan, McDonald's, and Sun Microsystems. And Tuesday, he informed the *New York Times*, through a reporter at SecurityFocus, that he had hacked into its corporate intranet, gaining access to employees' Social Security numbers and a source database that lists the phone numbers of the rich and powerful, including Rush Limbaugh, Jeanne Kirkpatrick, Jimmy Carter, and James Baker. Lamo says that for more than a week he had access to the personnel records of about 3,000 *New York Times* employees.

A *Times* spokeswoman says the company patched the holes after being notified of the problems by Lamo. "We take security extremely seriously," she says.

Lamo says he knows he's taking legal risks, but hacking into networks is part of his nature. "As long as unauthorized exploration is going to happen on some level, what makes the most sense to me is to have it harm the fewest people as possible. If I'm trying to push any idea for people to evaluate here, that's it. If you can't eliminate it, and possibly aren't sure you want to, is harm reduction so unreasonable?" he asks.

Lamo says he contacts the companies he hacks through the media because they don't "take calls from regular people seriously." When Lamo hacked into the networks of WorldCom and Excite@Home, both companies thanked him for finding the security problems and bringing them to their attention.

But some analysts say Lamo is simply a publicity seeker who causes more harm than good by exposing companies' security weaknesses. "He is like a drunk driver, and he doesn't understand the implication of his actions," says Pete Lindstrom, director of security strategies at Hurwitz Group. "Someone should take his notebook away."

Lamo said he broke into the newspaper's main intranet, or internal network, through another network linked to it. In all, he found seven insecure servers. He soon found an unsecured database of employee Social Security numbers, which he used to sign on to the system as various employees who were using the last four digits of their Social Security numbers as passwords, a common convention.

He then used the account of an administrative assistant to create a user account for himself with broad privileges.

Once he was signed on as an employee, he could have filed his own articles or possibly altered stories written by real New York Times reporters, **Lamo** acknowledged. He once changed an old news article archived on the Yahoo Web site to prove a point.

But tampering with New York Times stories "was something that I didn't think it was appropriate to explore," he said. Besides, he figured that the New York Times editors would stop any unauthorized writing from seeing print.

"I'd be surprised if any really heinous changes made it through," **Lamo** said.

E-mail Carrie Kirby at ckirby@sfchronicle.com.

LOAD-DATE: February 28, 2002

February 27, 2002 Wednesday

SECTION: Financial Pages

LENGTH: 235 words

HEADLINE: Hacker breaks into **New York Times**

DATELINE: SAN FRANCISCO, Feb 26

BODY:
A hacker is openly bragging he broke into a sensitive database at The **New York Times,** accessing sensitive information about employees and sources used by the prestigious newspaper.

In an article on the California-based SecurityFocus website, Adrian Lamo, a 21-year-old computer security consultant detailed how he used IP addresses to find a database containing employee social security numbers and other data. Using this information, he was then able to find a password that allowed him to access the paper's internal servers where he found contact information on sources and contacts used by the newspaper. Servers store and pass along data on a computer network.

"The server practically approached me," Lamo said in his critique of the newspaper's computer network.

Lamo boasted that he had accessed the home phone numbers and other records of the paper's roster of contributors to its opinion pages, including the personal information of Hollywood stars Warren Beatty and Robert Redford, former UN weapons inspector Richard Butler, conservative radio talk show host Rush Limbaugh and former president Jimmy Carter.

"We did get notified yesterday that there had been a security breach of our corporate security site," said Christine Mohan, a **New York Times** spokeswoman. "We identified the security flaw and addressed it."

Mohan said the newspaper is continuing to investigate the breach.

LOAD-DATE: February 27, 2002

Lamo said he's not trying to find such holes to make corporate computing safer but rather follows his interests to see what he can find. "There was no motive behind the act. I realize that some people will see my actions as illegal, immoral or worse," he said. "It's not for me to contest them or try to win them over to the Adrian Lamo school of security."

Skepticism from outsiders about his actions is "understandable," he said. "Any motive that I could tack onto it would just be justification that would be invalid ... to someone somewhere. There's never been a real reason behind it."

Pete Lindstrom, an analyst with Framingham, Mass.-based Hurwitz Group Inc., said he's puzzled that network intrusions by hackers like Lamo are often met with inaction by the companies whose information is exposed. "There's a Robin Hood aspect to this for some reason," he said. WorldCom's reaction to Lamo's December attack was to thank him, rather than prosecute him, Lindstrom said.

"I would love to know what the New York Times' CEO thinks since WorldCom [and others] forced his hand" by not taking previous legal action against Lamo, Lindstrom said. "This is a wayward kid who doesn't realize the impact of his actions. They need to take away his notebook and give him some real work to do."

Related stories:

- New York Times hit by Nimda worm variant, Nov. 1, 2001

- News sites simplified after performance bogs down, Sept. 11, 2001

- *Computerworld* coverage of viruses, worms and security holes

b6 -1,-2
b7C -1,-2

02/27/2002 12:19 PM

To:

cc:

Subject: AP, CNET, Reuters, MSNBC re: intranet hack

The **Associated Press**

The materials in the AP file were compiled by The **Associated Press**. These materials may not be republished without the express written consent of The **Associated Press**.

February 27, 2002, Wednesday, BC cycle

12:36 AM Eastern Time

SECTION: Business News

LENGTH: 197 words

HEADLINE: Hacker says he saw Social Security numbers inside New York Times' network

DATELINE: NEW YORK

BODY:
A San Francisco hacker says he found security lapses in The New York Times' internal computer network that exposed Social Security numbers for op-ed page contributors and other sensitive files.

Adrian **Lamo**, 21, a part-time Internet security consultant, said Tuesday that he hacked the newspaper's Web site and snooped around numerous times about 10 days ago. He said he found at least seven misconfigured servers, allowing savvy users to enter the newspaper's private network through its public Web site. He said he browsed through names and Social Security numbers of the paper's employees, home delivery customers' orders and contact information used by writers and editors on the Metro and Business desks.

He said he accessed a database of 3,000 contributors to the Times' op-ed page, which included Social Security numbers for celebrities and government officials.

Lamo said that the SecurityFocus Web site notified the newspaper of what he had done and that the newspaper patched the holes he found but did not acknowledge the incursion.

A telephone message left at the newspaper's corporate communications division was not

FBI(19-cv-1495)-1629

b6 -1,5,-2
b7C -1,5,-2

8

10

All the news that's fit to hack

Page Six.com

Richard Johnson

With Paula Froelich
and Chris Wilson

INTIMATE information about celebrity contributors to the New York Times op-ed page was exposed after a 21-year-old hacker broke into the paper's computer system.

It only took two minutes for security consultant **Adrian Lamo** to infiltrate the Times' internal network and get private poop on the likes of **Robert Redford, Warren Beatty, Jimmy Carter, William F. Buckley Jr., Rush Limbaugh, James Carville, James Baker** and **Jeanne Kirkpatrick.**

Lamo accessed a database of 3,000 contributors to the Times' opinion page that listed social security numbers, home telephone numbers, notes about how they feel about being edited, and how much they get paid.

He also accessed the names and social security numbers of all Times employees, lists of contacts used by the metro and business desks and logs of home delivery customers' start-and-stop orders.

"The server practically approached me," Lamo bragged to SecurityFocus.com. The crafty computer whiz discovered seven servers acting as doorways between the public Internet and the Times' private intranet, making the information available to anyone capable of properly configuring a Web browser.

Lamo notified the Times of its porous database on Tuesday. In a statement, a red-faced Times spokesperson said: "We are actively investigating a potential security breach. Based on the results of this investigation we will take appropriate steps to ensure the security of our network."

Lamo has earned a reputation for hacking into the networks of large corporations, alerting the companies and offering to fix their vulnerabilities — for a price.

In December, he was praised by communications monolith WorldCom after he discovered — and helped fix — gaping holes in its intranet that threatened to expose the private networks of Bank of America, Citicorp and J.P. Morgan.

A few months earlier, he had shown how easy it was to hack into a Yahoo! News Web site by tampering with a wire service story posted on the site. At least Lamo was unable to tinker with Times stories before they got into print. The paper's Web site is not tied in to its Swiss cheese-like internal computer system.

Last year, anti-globalization activists hacked into a World Economic Forum database and downloaded details about **Bill Clinton, Bill Gates,** South African President **Thabo Mbeki** and Japanese Prime Minister **Yoshiro Mori,** all attendees of the group's summit in Davos, Switzerland.

Steve's gains

LAST week was good for author **Steven Gaines.** First, Penguin signed a deal to re-release his best-selling 1984 Beatles bio, "The Love You Make." Days later, HBO announced it was making his 1991 tell-all "Simply Halston" into a movie. Strangely, the two names most commonly dropped to play the Midwest-born designer are Brits, **Jeremy Irons** and **Rupert Everett.** But spies say Irons thinks he's too old for the part while Everett doesn't think he could pull off Halston's twang. We nominate **Gary Oldman.**

Sightings

HUGH Grant speeding up and then ducking into the Rizzoli bookstore to get away from...

about a potential security breach of our corporate intranet site," she said.

"We identified the security flaw and addressed it," Mohan said. "We are continuing to investigate the situation to ensure the security of our network."

This isn't the first time the newspaper has come under attack; in 1998 a hacker posted pornography and racist text on the newspaper's Web site.

===

MSNBC.com

N.Y. Times source database hacked

Paper's rich-and-famous op-ed, source database revealed

By Bob Sullivan
MSNBC

Feb. 27 — A computer security researcher accessed internal New York Times computer networks this week through the Internet and managed to view hundreds of sensitive Times files. Among them: a database of 3,000 Times op-ed page contributors. The file contained Social Security numbers and other personal information belonging to luminaries like James Carville, James Baker, Larry Lessig, and Robert Redford. The researcher also got phone numbers for William F. Buckley Jr., Rush Limbaugh, Warren Beatty and Jimmy Carter. In a statement , the New York Times said it is investigating the problem.

THE RESEARCHER, ADRIAN LAMO, has a long history of exposing computer security problems at major Web sites. In the past, he has uncovered problems with America Online's Instant Messenger, with MCI WorldCom networks that services big-name clients like Bank of America, and at Yahoo! When he breached Yahoo's security, Lamo was able to alter the content of a news story and post it on the Web portal's site.

Lamo said he wasn't about to access New York Times content when he rummaged through the company's network earlier this week. But he was able, with relative ease, to poke around the Times' corporate networks. While there, he was able to see names and social security numbers of Times employees, home delivery logs, even source lists for the newspapers' reporters.

Lamo said he informed the newspaper of the breach through Kevin Poulsen, a reporter at computer security news Web site SecurityFocus.com, on Tuesday.

In a statement, the New York Times said it is investigating Lamo's claims.

"The New York Times Company takes the security of its network very seriously," said spokesperson Christine Mohan. "Yesterday, we were notified about a potential security breach of our corporate intranet site, we identified the security flaw and addressed it. We are continuing to investigate the situation to ensure the security of our network."

Lamo supported his claims with a variety of screen shots sent to MSNBC.com. The images show lists names from what appear to be internal New York Times databases. Lamo was even able to add his name and phone number to a database of experts used by Times' reporters.

The researcher said he was able to access the Times' networks simply through a Web browser by locating vulnerable New York Times "proxy" servers. Proxy servers are generally considered a tool of safety, acting as a bridge between a company's internal network and the

outside world. But if they are misconfigured, they act instead as the perfect place to launch an attack. Once Lamo accessed a Times proxy server, he was able to hunt and peck through private information belonging to Times' employees and customers.

"This surely wasn't anything the people involved had counted on when they'd been filling out that tell-us-about-yourself account form," he said.

Lamo, a 21-year-old nomad who is among the few computer researchers that use their real name when informing a company about a security problem, said he generally does his work to improve the state of computer security at large companies. His unconventional tactics are frequently criticized, he says.

"I recognize that some people will see my actions as illegal, immoral, or worse. It's not for me to contest them or try to win them over to the Adrian Lamo School of Security," he said. "I've done my best to act in good faith and avoid harm to the company and employees involved."

New York Times Intranet, Source Database Hacked

By Brian Krebs, Newsbytes
WASHINGTON, D.C., U.S.A.,
26 Feb 2002, 7:52 PM CST

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE ___ BY [   ] BAW:TJ:BJS

b6   1
b/C   1

The New York Times' corporate Intranet and Web-based applications that handle everything from payroll accounts to the newsroom's source database were penetrated by a freelance security researcher this week using nothing more than a Web browser, Newsbytes has learned.

The discovery was made by 21-year-old Adrian Lamo, a white-hat hacker known for tracking down and alerting Fortune 500 companies that employ lackluster or non-existent security measures on their Web sites.

The internal Web site included pages with detailed instructions for stringers and correspondents on how to file from the field, complete with dial-in modem numbers and accounts. The intranet also lists each Times employee's contact information, as well as their Social Security numbers.

According to screenshots obtained by Newsbytes, the Times' own "Everyone, Everywhere" newsroom contact database was also available via the corporate Intranet. The database contains phone numbers and contact information for such household names such as Yogi Berra, Warren Beatty, and Robert Redford, as well as high-profile political figures - including Palestinian leader Yassir Arafat and Secretary of State Colin Powell.

The source database also contains Social Security numbers for all of the Times' guest op-ed writers, including Democratic operative James Carville and Internet policy guru Lawrence Lessig. Also spotted in the file were entries for William F. Buckley Jr., Rush Limbaugh, Microsoft founder Bill Gates, and New York Mayor Michael Bloomberg.

In September 1998, a hacker group known as "Hacking for Girlies" broke into the New York Times Web site, replacing the main page with its insignia and a lengthy diatribe against New York Times technology columnist John Markoff for his book "Takedown," which the group said painted an inaccurate picture of hacker icon Kevin Mitnick.

The New York Times subsequently moved the servers for its public Web sites to a more secure Internet address block.

But the company left many Web pages created for use by employees and field reporters open to just about anyone curious enough to look for them, Lamo said.

Times spokeswoman Christine Mohan confirmed that the company is "actively investigating a potential security breach.

"The New York Times Company takes the security of its network very seriously," Mohan said. "Based on the results of this investigation, we will take appropriate steps if necessary to ensure the security of our network."

Lamo located the internal network after querying publicly accessible Internet address records for mail servers on the New York Times address space, armed with the knowledge that e-mail is often processed by the same systems and networks that manage a corporation's firewall.

Lamo gained access to the network using Web proxies located on the network. Proxies are machines that allows users to route through - or into - networks, often skirting past firewalls. The whole process from search to discovery took less than two minutes.

"It struck me as being a part of their network more likely to be placed in a trusted location," he said.

"Ironically, it wasn't until I mistyped a URL that I found what I was looking for - the error message invited me to 'try the main New York Times intranet site' instead."

The Times' corporate intranet also allows users to access other sensitive areas, including the company's human resources department, as well as tools used to submit advertisements that accompany stories in the daily paper and the New York Times Web site, http://www.nytimes.com .

The discovery highlights just how susceptible the Internet can be as a tool for spreading misinformation. Lamo said had he been so inclined, he probably would have been able to figure out how to successfully submit a small news item or advertisement for publication.

Days after the Sept. 11 attacks, Lamo used a proxy on the Yahoo network to add satirical comment to a story on the company's Web site about Russian programmer Dmitry Sklyarov, a stunt that raised public concern about the integrity of online media.

Last week, Lamo alerted SBC Communications that several of its Web pages containing tens of thousands of subscriber user names and passwords were exposed to the Web and completely unprotected.

In December, Lamo discovered an Internet-accessible Web tool that provided easy access to the keys to private network routers for dozens of companies, including AOL Time Warner, Bank of America, Citicorp, Fox News Corp., JP Morgan, McDonalds, and Sun Microsystems - to name just a few.

When asked why he does what he does, Lamo is noncommittal and somewhat cagey, downplaying his penchant for seeing things in ways that often go unnoticed by most.

That didn't stop him, however, from quietly adding his name to the newsroom's source list as an expert on computer hacking.

"I'm not trying to bring about any sort of specific change anywhere by what I do - but in doing what I do, acting in good faith doesn't seem like a bad thing, and hoping that someone in a similar situation in some undefined future might have options that aren't all a downwards spiral doesn't seem unreasonable either," Lamo said. "It would be nice."

Reported by Newsbytes.com, http://www.newsbytes.com

19:52 CST
Reposted 19:57 CST

(20020226/WIRES ONLINE, LEGAL, BUSINESS, TELECOM/NYTIMES/PHOTO)

2

b6 -1,2
b7C -1,2

02/27/2002 10:53 AM

To:
cc:

Subject: AP article on Hacker

<div align="center">

The **Associated Press**

</div>

The materials in the AP file were compiled by The **Associated Press.** These materials may not be republished without the express written consent of The **Associated Press.**

<div align="center">

February 27, 2002, Wednesday, BC cycle

12:36 AM Eastern Time

</div>

SECTION: Business News

LENGTH: 197 words

HEADLINE: Hacker says he saw Social Security numbers inside New York Times' network

DATELINE: NEW YORK

BODY:
A San Francisco hacker says he found security lapses in The New York Times' internal computer network that exposed Social Security numbers for op-ed page contributors and other sensitive files.

Adrian **Lamo,** 21, a part-time Internet security consultant, said Tuesday that he hacked the newspaper's Web site and snooped around numerous times about 10 days ago. He said he found at least seven misconfigured servers, allowing savvy users to enter the newspaper's private network through its public Web site. He said he browsed through names and Social Security numbers of the paper's employees, home delivery customers' orders and contact information used by writers and editors on the Metro and Business desks.

He said he accessed a database of 3,000 contributors to the Times' op-ed page, which included Social Security numbers for celebrities and government officials.

Lamo said that the SecurityFocus Web site notified the newspaper of what he had done and that the newspaper patched the holes he found but did not acknowledge the incursion.

A telephone message left at the newspaper's corporate communications division was not immediately returned Tuesday night.

LOAD-DATE: February 27, 2002

FBI(19-cv-1495)-1635

...e checking the doors, and

		+ = posi
1 = significant mention of NYTCO		= nega
2 = passing mention of NYTCO		N = neut
3 = industry article		

BusinessWeek online
Business Solutions Directory

BusinessWeek online

MARCH 5, 2002

SECURITY NET
By Alex Salkever

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-10-2010 BY [   ]UC BAW/DK/RS

Close Window

DO -1
b7C -1

Stop Him Before He Hacks Again

Adrian Lamo has made quite a name for himself by breaking into corporate networks. He has done no harm -- but that's not the issue

Readers of _The New York Times_'s "op-ed" page regularly find columns written by a host of world leaders and celebrities, from Palestinian leader Yassir Arafat and former U.S. President Jimmy Carter to hip-hop star and talk-show host Queen Latifah. The contact information for these luminaries is a closely guarded _Times_ secret, as is the contents of the op-ed section's Rolodex.

Not anymore. The _Times_ op-ed section and its list of contributors were recently penetrated by one of the most controversial hackers to emerge since Kevin Mitnick, who spent almost five years in prison for repeatedly invading computer systems at a slather of high-tech outfits. Meet Adrian Lamo, a soft-spoken 21-year-old snoop from San Francisco who hacks with nothing more than a laptop, a Web browser, and a Net connection at the local coffee shop.

FRIENDLY WARNING. Lamo recently broke into the _Times_ computer network, where he co-opted contact-information files as well as sensitive details of the news-gathering and editing process at the _Times_. His tear through the Gray Lady's closet even gave him the ability to change the Web site at one of the world's most powerful media organizations with a few key strokes -- an option he didn't exercise. Lamo then contacted computer-security publication _Security Focus Online_ and asked it to contact the _Times_ on his behalf to outline the breach.

This isn't Lamo's first conquest. In September, 2001, he hacked into the content servers at Yahoo! -- and actually did alter a news story to demonstrate that he was capable of breaching security. A month later, he acked customer-information databases at software powerhouse Microsoft. In December, 2001, he gained access to secret network-topography diagrams at voice-and-data carrier WorldCom, going so far as to e-mail company officials a supposedly secret file showing key locations of network equipment.

why hasn't Lamo been prosecuted for computer crimes? In each of these cases, he warned the companies out their flaws after-the-fact and offered to help fix them for free. Lamo further claims that he has accepted money or compensation from any of his targets, something that often happens in the computer-security rld, where a consultant reporting a breach often gets awarded a contract. Rather than condemning him, no's "victims" have mostly praised him for helping to secure their networks.

RUDER OR HERO? So far, the _Times_ has neither condemned nor lauded Lamo. "We are currently deter... t the appropriate next steps will be," was how _Times_ spokesperson Christine Mohan responded to BusinessWeek Online. To date, no one has pressed charges.

indow

A Star Is Born, Security Suffers

Pete Lindstrom, Director, Security Strategies
December 7, 2001
Hurwitz TrendWatch — Thinking Out Loud

Yesterday, we were all witness to the worst case of security apathy in the public world. If I had seen this in a movie, I'd have walked out because the plot was just too unbelievable. A 20 year-old "do-good" hacker poked and prodded his way into one of the largest networks in the world, owned by WorldCom, gained access to all sorts of information that was apparently considered insignificant, and by the end of the story the WorldCom team is THANKING him for it. It is enough to make me retch.

The Incident

So the "wandering" dumpster diver, Adrian Lamo, apparently used a widely-available hacker tool to find a hole in WorldCom's network and proceeded to masquerade as an insider. Reportedly, he spent a month getting access to highly detailed diagrams of WorldCom's physical network infrastructure, employee records (with claims to be able to change an employee's direct deposit information), and passwords to gain access to the networks of WorldCom's client companies like Bank of America, JP Morgan, Citicorp, Sun Microsystems, and AOL (I sure hope they are screaming). Then he confessed.

The Response

Apparently, when WorldCom found out, they all got together to make nice. He willingly signed a non-disclosure agreement and showed the WorldCom folks their security vulnerability. They proceeded to SHOWER HIM WITH PRAISE like "We really appreciate his efforts to work with us" and asserted "At that end of the day, what he did wasn't destructive or harmful." This last comment, of course, is the key indicator that WorldCom has NOT LEARNED ITS LESSON.

The Resolution

Whew! I suppose it is over and everyone can go home happy. Lamo got the attention he wanted, WorldCom got a 20-year-old hacker's seal of approval, and security professionals around the world got a slap in the face.

Why is it that we scream about rogue viruses and ignore a hacker with free reign over one of the biggest telecom company's intranet? Let me be clearer: I am absolutely astounded at the indifference, nay graciousness, with which a company like WorldCom is treating the hacking nomad, Adrian Lamo, after he spent a month

"doing nothing wrong" on its internal network. Given the reported information, this is the most extreme case of negligence I have ever seen.

Mistakes happen to even the most diligent enterprises. But to dismiss the nature of this CRIME screams negligence. Lamo broke the law, confessed, and was given a pat on the back. WorldCom claims nothing significant occurred. Nobody learned here.

WorldCom can't really be sure there was no damage unless it does a thorough review of every network device and host system accessible via its Internet and changes all passwords associated with administration. The fact that it doesn't seem to think the incident is significant indicates that it won't perform these procedures.

How many ways can something as benign as this go wrong? Let's see, what if he makes a mistake? What if someone steals his laptop? What if he stops liking you? What if he gives away the stuff he kept? What if he comes back? What if he uses that access to gain access to another site? There are too many possibilities that can lead to something going wrong.

There are a number of victims here, including under-appreciated customers and denigrated WorldCom security employees. These victims should strongly consider the impact of this incident as well as the precedent it sets.

Adrian Lamo is a "serial hacker" looking for press who doesn't think he is doing anything wrong. What he deserves is jail time. WorldCom is a negligent entity that has breached the trust of all of its customers. What it deserves is a class-action lawsuit. The entire incident is indicative of the apathy that runs rampant in the face of actual incidents.

Adrian Lamo's Reported Victims:

AOL, Apple Computer, Journal of Commerce, Microsoft, Excite@Home, Yahoo, World Bank, WorldCom, WorldCom Customers (Bank of America, JP Morgan, Citicorp, Sun Microsystems).

Adrian Lamo's Quotes (All from SecurityFocus):

"The downside is, I'm running out of major U.S. corporations."

"For me, [WorldCom's intranet is] a massive playground that's slowly and inexorably crumbling away at their security infrastructure."

"I made it clear very quickly that all I was interested in doing was make it as positive an experience as possible for everyone."

"I do what I do, there's no particular motive I can describe."

UPD

UPLOADED
WITH/TEXT ✓
WITHOUT TEXT
BY
DATE 6-12-02

SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____

JUN 1 0 2002

b6 -1,2
b7C -1,2
b3 -2
b7E -3

FD-302 (Rev. 10-6-95)

b6   1
b7C   1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   02/28/2002

[   ] THE NEW YORK TIMES,
telephone number [   ] was telephonically contacted by
the interviewing agent. After being advised as to the identity of
the interviewing agent and the purpose of the interview, [   ]
provided the following information:

[   ] is aware of an unauthorized computer intrusion
into THE NEW YORK TIMES' intranet by ADRIAN LAMO. LAMO announced
to the media that he had hacked THE NEW YORK TIMES. [   ]
confirmed that LAMO gained unauthorized access to their intranet
and added his name to a newsroom database. LAMO also, gained
access to their circulation area and a database that contained the
names of their employees. LAMO was able to crack the password of
one of their former employees. The former employees userid had
supervisory rights. Using the supervisory rights, LAMO created
other userid's on the network.

b6   2
b7C   2

[   ] commented that LAMO was also able to gain
access to a beta database.

Investigation on	02/27/2002	at New York, NY	(telephonically)

File # [   ]   Date dictated   02/28/2002

by   SA [   ]

b6   1
b7C   1
b7E   2

FBI(19-cv-1495)-1640

wpt

b6 -1,2
b7C -1,2
b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-__-2010 BY [   ] UC BAW DK RYS

b6   1
b7C   1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   06/10/2002

[   ]

THE NEW YORK TIMES(TIMES), 229 West 43rd Street, New York, NY
10036, telephone number [   ] was interviewed at his
place of employment. Also present during the interview was [   ]
[   ] After being advised as
to the identities of the interviewing agents and the purpose of the
interview, [   ] provided the following information:

          In February 2002, [   ] was informed that an
individual by the name of ADRIAN LAMO hacked into the TIMES'
intranet. While reviewing the monthly activity of their Lexis-
Nexus accounts, [   ] noted that two (2) accounts; [   ]
and [   ] utilized approximately 18% of the total usage by
THE NEW YORK TIMES for the month. THE NEW YORK TIMES pays a flat
fee for Lexis-Nexus services except in special circumstances.

          [   ] explained that [   ]
[   ]
[   ]
[   ]
[   ]
[   ]. When [   ]
saw the monthly usage for the [   ] and [   ] accounts he became
curious. [   ] queried several individuals to determine if they
were employees of the TIMES. [   ] confirmed that the
individuals were not employees, former employees or freelancers of
the TIMES.

          [   ] contacted [   ]
[   ] Lexis-Nexus, telephone number [   ]
stated that a Lexis-Nexus investigation revealed that the accounts
were being accessed from two (2) KINKO's locations in California.
It was Lexis-Nexus belief that the TIMES' network had been hacked
and there were three accounts created at that time. [   ]
provided [   ] with the dates and times the accounts were
created and the accounts were disabled. [   ] further stated
that [   ]

b6 -1,2
b7C -1,2

b6 -,5
b7C 2,5
b7E 2

b3 -2
b6 -1
b7C -1
b7E -3

Investigation on   06/06/2002   at   New York, NY

File # [   ]

Date dictated   06/10/2002

SA [   ]
by SA [   ]

FBI(19-cv-1495)-1642

[   ] commented that also through the newsroom
intranet the employees are able to access [   ]
[   ] the employees are able to create
new userids and passwords like for Lexis-Nexus. [   ] stated he
contacted an individual at [   ] whose name he currently does not
remember. To date investigation into whether any accounts were
created [   ] by LAMO are negative.

[   ] provided an email that contains the account
information for the accounts set up by an unauthorized user.

wpd

UPLOADED

WITH TEXT ✓

WITHOUT TEXT

BY (a)

DATE 6-12-02

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED.
DATE 2-?-? BY [ ] ?? BAW?: ?.S

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   06/10/2002

[ ] THE NEW
YORK TIMES, 229 West 43rd Street, New York, NY 10036, was
interviewed at his place of employment. Also present during the
interview was [ ] THE
NEW YORK TIMES. After being advised as to the identities of the
interviewing agents and the purpose of the interview, [ ]
provided the following information:

b6 ?
b7C 2

[ ] is aware of the unauthorized access of THE NEW
YORK TIMES' network by ADRIAN LAMO. LAMO accessed their intranet
via a proxy server. The proxy server was configured to allow
proxy's to occur for operational purposes. [ ] explained
that the proxy server redirects to the web servers and firewalls.
Once LAMO gained unauthorized access their proxy server, he
configured his web browser to be their proxy server. By doing this
any activity he performed on their network was trusted because the
proxy server was a trusted machine. [ ] further commented
that LAMO was able to determine which one of their proxy servers
were vulnerable by using a program called a proxy hunter.

When [ ] was informed that LAMO had hacked into
their network, [ ]
[ ] was able to see what areas/links LAMO had access to.

b6 -2
b7C -2
b7E -2

One (1) of the servers that LAMO was able to view was the
newsroom server. LAMO had full access to this server after he
became the proxy server. It was through this server that LAMO was
able to set up Lexis-Nexus accounts as well as manipulate other
databases.

[ ] stated that steps have been taken to prevent a
similiar hack occurring to THE NEW YORK TIMES.

Investigation on   06/06/2002   at   New York, NY

File # [ ]   Date dictated   06/10/2002

by   SA [ ] :cah

b3 -2
b6 -1
b7 -1
b7E -3

FBI(19-cv-1495)-1645

C 37

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 09/20/02   Time: 13:39

Case ID: [ ]

Description of Document:

    Type : OTHER
    Date : 05/22/02
    To   : NEW YORK
    From : [ ]
    Topic: [ ] INTERNET MESSAGE

Reason for Permanent Charge-Out:

    inadvertently filed

Transferred to:

    Case ID: [ ]

    Employee: [ ]

b6 -1,5
b7C -1,5
b3 -2
b7E -3

b3 -2
b7E -3

FBI(19-cv-1495)-1646

UPLOADED

WITH/TEXT ✓

WITH/OUT

BY

DATE 8-20-02

AUG 1 0 2002

b3   2
b6   1
b7C   1
b7E   3,4

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 08/16/2002

To: New York   Attn: C-37

From: New York
      Squad C-37
      Contact: SA [ ]

Approved By: [ ]

Drafted By: [ ] slf

Case ID #: [ ]

Title: ADRIAN LAMO;
       New York Times-Victim;
       Computer Intrusion;
       OO:NY

Synopsis: Request investigative research assistance with
analysis [ ] of ADRIAN LAMO.

Enclosure(s): One (1) copy of [ ] of ADRIAN   b6 4
LAMO for the dates of 6/1/01-5/7/02.

Details: In February 2002, LAMO discovered several misconfigured
proxy servers acting as doorways between the public Internet and
the New York Times' private intranet. LAMO utilized the proxy
servers to gain access to the New York Times network. Once on
the network, LAMO cracked a password for a userid with supervisor
rights. Utilizing this userid he was able to broaden his access
as well as perform certain functions within the network. LAMO
had access to individuals names and Social Security Numbers.
LAMO informed The New York Times of the security vulnerability
through SECURITYFOCUS.COM.

     LAMO has committed computer intrusions into several
other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME
and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for
proxy servers that are misconfigured. Once he obtains this
information, he configures his browser to appear and utilize the
proxy server as his own. Once the computer intrusion occurs,
LAMO searches the network to determine if there are any other
vulnerabilities and in the case of The New York Times, left a
backdoor so that he could enter at another time undetected.

     Each time LAMO commits a computer intrusion on a high
profile organization he reports the vunerability and intrusion to

b3   b7E

the media causing a distrust of the company's clients.   The above
mentioned corporations have lost significant money and trust of
their clients.

        Pursuant to a subpoena request, writer received the

          Investigation has revealed that LAMO has provided
unauthorized access to Lexis-Nexus account to individuals he
knows in California, Utah, Colorado and Atlanta.   A brief review
of
                              On 8/16/02, writer requested subpoenas
from AUSA   for

b3 -4
b6 -4
b7C -4

        Writer requests assistance in analysis of the enclosed
          ADRIAN LAMO.

b3 -2
b7E -3

LEAD(s):

Set Lead 1: (Adm)

NEW YORK

AT NEW YORK

Request for the assistance of NYO IOS in the above
mentioned investigation.

♦♦

3

FBI(19-cv-1495)-1650

16
Precedence: ROUTINE   Date: 8/29/2002

To: Counterterrorism   Attn: Computer Investigations
                                     Unit, CIOS, NIPC,
                                     Room 11719

From: SAC, Dallas

Approved By: [_____]

Drafted By: [_____]al

Case ID #: [_____]

Title: Subject: Adrian Lamo
        Victim: Southwestern Bell - Victim
        Type: Computer Intrusion
        Date: 8/29/02

SUBMISSION: X Initial   Supplemental X Closed

CASE OPENED: 08/29/2002

CASE CLOSED: 8/29/2002
   ● No action due to state/local prosecution (Referred to Dallas Police Department, LT[_____])
   ● SA declination
X Referred to Another Federal Agency (Name/Number:FBI New York [_____])
   Placed in unaddressed work
   Closed administratively
   Conviction

COORDINATION: FBI Field Office   __New York_____
                  Government Agency   _____
                  Private Corporation _____

Case ID [_____]   Serial [_____]

OCT 0 [ ] 2002

b6   1
b7C   1
b3   2
b7E   3

b3 -2
b6 -1,7
b7C -1,7
b7E -3

VICTIM

Company name/Government agency: Southwestern Bell Corporation, 1701   b6 -2
Alma Drive, Plano, TX, POC [   ]   b7C -2

Purpose of System: Telecommunications
Highest classification of information stored in system: Unclass.

System Data:
        Hardware/configuration (CPU): Network
        Operating System: Multiple
        Software:

Security Features:
        Security Hardware Installed: X yes   no
        Logon Warning Banner: yes   no

                INTRUSION INFORMATION

Access for intrusion: X Internet connection   dial-up number   LAN (insider)
        If Internet: Internet address:
                        Network name:

Method:
        Technique(s) used in intrusion: Unknown

of intrusion: N/A
        addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
        country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
        facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject: Adrian Lamo
        Age: Race:
        Sex: Education: _____
        Alias(s): _____ Motive: __Financial Gain_____
        Group Affiliation: _____
        Employer: _____.
        Known Accomplices:
        Equipment used:
                Hardware/configuration (CPU): _____

Operating System: _____

Software: _____

Impact:

Compromise of classified information: yes X no

Estimated number of computers affected: Unknown

Estimated dollar loss to date: Unknown

Category of Crime:

Impairment: Theft of Information:

Malicious code inserted

●ified information compromised

Denial of service

Unclassified information compromised

Destruction of information/software   Passwords obtained

Modification of information/software   Computer processing time obtained

Telephone services obtained

Application software obtained

Operating software obtained

Intrusion:

Unauthorized access

Exceeding authorized access

REMARKS

On 8/28/02, Dallas was contacted telephonically by|_____|
|_____| Security, Southwestern Bell Corporation, Dallas, TX, |_____|
|_____|stated that he had been reading an article on
security focus regarding Lamo not appearing on NBC for a piece
NBC was doing regarding hacking when|_____|noticed that Lamo took
credit for being inside of a Telecom company.

|_____|informed Dallas that this might have been his
company. |_____|stated that shortly before this, his company had
received an e-mail from Lamo informing them that they were
vulnerable, but added that this had never been followed up on.
|_____| was unaware of any losses or of any compromised systems, and
based his contact with the FBI solely on the e-mail from Lamo.
Dallas recalled that Dallas had previously covered leads
regarding Worldcom at Dallas in relation to Lamo for New York.
Dallas therefore referred|_____|to New York, and in particular SA

bo 2
b7   ·

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 08/29/2002

To: New York   **Attn:** C-37
                                          SA [   ]
       Dallas

From: Dallas
        Cyber Squad
        Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ]:al

Case ID #: [   ]

b6 -1
b7C -1
b3 -2
b7E -3

Title: ADRIAN LAMO
        New York Times-Victim;
        Computer Intrusion;

Synopsis: Claim statistical accomplishment and refer victim to New York.

Details: On 8/28/02, Dallas was contacted telephonically by [   ]
[   ] Security, Southwestern Bell Corporation, Dallas, TX, [   ]
[   ] stated that he had been reading an article on
security focus regarding Lamo not appearing on NBC for a piece
NBC was doing regarding hacking when [   ] noticed that Lamo took
credit for being inside of a Telecom company.

[   ] informed Dallas that this might have been his
company. [   ] stated that shortly before this, his company had
received an e mail from Lamo informing them that they were
vulnerable, but added that this had never been followed up on.
Dallas recalled that Dallas had previously covered leads
regarding Worldcom at Dallas in relation to Lamo for New York.
Dallas therefore referred [   ] to New York, and in particular SA
[   ]

b6 -1,2
b7C -1,2

SEARCHED _____ INDEXED _____
SERIALIZED _____ FILED _____

SEP 2 0 2002

FBI - [   ]

b3   2
b6   1
b7C 1
b7E 3

FBI(19-cv-1495)-1654

b3 -2
b7E -3

Accomplishment Information:

Number: 1
Type: [   ] VICTIM CONTACTED/INTERVIEWED
ITU:
Claimed By:
    SSN:
    Name: [   ]
    Squad: Cyber

b6   1
b7C   1
b7E   5

Number: 1
Type: [   ] SUBJECT IDENTIFIED
ITU:
Claimed By:
    SSN:
    Name: [   ]
    Squad: Cyber

b3 -2
b7E -3

LEAD(s):

Set Lead 1:   (Adm)

NEW YORK

AT NEW YORK

For information of New York.

♦♦

3

LEAD/ASSIGN/COVERED
DATE
ASSIGN TO
SUPV

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-15-__ BY __ BAW : B.S

b5   2
b6   1
b/C   1
b/E   3

Precedence: ROUTINE   Date: 08/29/2002

To: New York   Attn: C-37
                                   SA [   ]

    Dallas
                                            ALL INFORMATION CONTAINED
                                            HEREIN IS UNCLASSIFIED
From: Dallas   DATE 13-__-____ BY [   ] U: ___ __ R__
       Cyber Squad
       Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ]al   b3 -2
                                                       b6 -1
Case ID #: [   ]   b7C -1
                                                       b7E -3

Title: ADRIAN LAMO
       New York Times-Victim;
       Computer Intrusion;

Synopsis: Claim statistical accomplishment and refer victim to
New York.

Details: On 8/28/02, Dallas was contacted telephonically by[   ]
[   ] Security, Southwestern Bell Corporation, Dallas, TX, [   ]
[   ]stated that he had been reading an article on
security focus regarding Lamo not appearing on NBC for a piece
NBC was doing regarding hacking when[   ]noticed that Lamo took
credit for being inside of a Telecom company.

      [   ]informed Dallas that this might have been his   b6 1,2
company. [   ]stated that shortly before this, his company had   b7C 1,2
received an e-mail from Lamo informing them that they were
vulnerable, but added that this had never been followed up on.
Dallas recalled that Dallas had previously covered leads
regarding Worldcom at Dallas in relation to Lamo for New York.
Dallas therefore referred[   ]to New York, and in particular SA

 [   ]

 Accomplishment Information:

Number: 1
Type:[   ]VICTIM CONTACTED/INTERVIEWED
ITU: [   ]   b3 -2
Claimed By: b6 -1
    SSN: [   ]   b7C -1
    Name: [   ]   b7E -3,5
    Squad: Cyber

Number: 1

Case ID : [   ]   Serial : [   ]

Type: [   ] SUBJECT IDENTIFIED
ITU:
Claimed By:
  SSN: [   ]
  Name: [   ]
  Squad: Cyber

b6 -1
b7C -1
b7E -5

 LEAD(s):

Set Lead 1: (Adm)

    NEW YORK

     AT NEW YORK

     For information of New York.

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 09/09/02   Time: 13:21

Case ID: [   ]

Description of Document:

    Type : FD801
    Date : 08/27/02
    To   : COUNTERTERRORISM
    From : DALLAS
    Topic: KTNT-VICTIM

Reason for Permanent Charge-Out:

    serialized to the wrong case file by mistake.

Transferred to:

    Case ID: [   ]

Employee: [   ]

b6   1
b7C   1
b5   2
b7E   3

FBI(19-cv-1495)-1660

b5   2
b7E   3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-19-__ BY [ ] U BAW/DI K/S

FEDERAL BUREAU OF INVESTIGATION

Date of transcription ___09/11/2002___

In connection with the pending investigation, and in concurrence with Assistant United States Attorney [   ] the writer [   ] with subject ADRIAN LAMO

bc 1,4
b7C 1,4
b7E 1,4

Subsequently, the writer [   ] [   ] and is being submitted to the 1A section of this case file with this communication. A copy of this

SEARCHED ___ FILED ___
SERIALIZED ___

SEP 1 1 2002

FBI — NEW YORK

Investigation on ___9/6/2002___ at New York, NY

File # [   ]

by SA [   ]

Date dictated ___

b3 -2
bc -1,5
b7C -1,5
b7E -3

BY [   ]
DATE 9-13-02

FBI(19-cv-1495)-1661

Kinkoid.wpd

UPLOADED
WITH/TEXT ✓
WITH[ ]
BY
DATE 9-13-02

(Rev 08-28-2000)

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY   Date: 09/06/2002

To: Washington Field   Attn: Squad CT8
                                         SSA _____

      Philadelphia   Attn: Squad 9
                                         SSA _____

      San Francisco   Attn: Squad 14B
                                         SSA _____

From: New York
         Squad C-37
         Contact: SA _____
                   cellular telephone _____

Approved By: _____

Drafted By: _____ slf

Case ID #:   _____

b3 -2
b6 -1
b7 -1
b7E -3

Title: ADRIAN LAMO;
        New York Times-Victim;
        Computer Intrusion;
        OO:NY

Synopsis: Determine if ADRIAN LAMO has utilized listed Kinko's
           facilities

Enclosure(s): Listing of Kinko's facilities in Washington, DC
               Listing of Kinko's facilities in Philadelphia, PA
               Listing of Kinko's facilities in San Francisco, CA

               One (1) copy recent news story about LAMO with
               photo

Details: In February 2002, LAMO discovered several misconfigured
proxy servers acting as doorways between the public Internet and
the New York Times' private intranet. LAMO utilized the proxy
servers to gain access to the New York Times network. Once on
the network, LAMO cracked a password for a userid with supervisor
rights. Utilizing this userid he was able to broaden his access
as well as perform certain functions within the network. LAMO
had access to individuals names and Social Security Numbers.
LAMO informed The New York Times of the security vulnerability
through SECURITYFOCUS.COM.

          LAMO has committed computer intrusions into several
other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME

and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

LAMO is a vagrant, traveling by bus from the East Coast to the West Coast and vice versa staying with friends or in hostels. LAMO utilizes the services of Kinko's to perform the majority of his hacking with his Toshiba laptop. LAMO is not employed, therefore when he performs his hacking he may spend hours at Kinko's.

Each time LAMO commits a computer intrusion on a high profile organization he reports the vulnerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

On approximately August 22 2002, LAMO hacked into NBC and a telecommunications company while being taped by a reporter for NBC to be aired on NBC Nightly News. The story was pulled when NBC attorney's learned of its content. LAMO committed the hacks from a Kinko's store on the East Coast. LAMO gained unauthorized to the telecommunications companies network and it unsure at this time whether he had authorization to hack into NBC's network. The New York Office is investigating this unauthorized access further.

b7E 1

LAMO also has ties to former hacker [   ] who was arrested by the FBI for computer intrusion/national security charges. [   ] for LAMO and the corporations he hacks. [   ]

b6
b7C

The New York Office and the Southern District of New York are currently investigating LAMO and his computer

2

intrusions. The NYO along with the SDNY are looking to have an
indictment against LAMO by the end of September.

Descriptive Data:

```
        Name -
        Last:           LAMO
        First:          ADRIAN
        Middle:
        Race:           W
   Sex:                 M
   SOC:                 042-74-6804
   Address -
        House #:        1230
        Street Name:    Market Street, #106
        City:           San Francisco
        State:          CA
        Postal Code:    94102
```

3

b3 -2
b7E -3

LEAD(s):

Set Lead 1:

WASHINGTON FIELD

AT WASHINGTON, DC

Interview all employees of the following Kinko's stores and conduct logical investigation. Determine the ip address range allocated to the store for internet access, if not dynamically assigned. Determine the store's internet access and logging procedures. If LAMO is at any of the below listed locations, contact writer immediately.

Kinko's locations:

1. Washington DC 7th & D
   325 7th Street
   Washington, DC 20004-2801
   (202) 544-4796

2. Washington DC Capital Hill
   317 Pennsylvania Ave SE
   Washington, DC 2003-1148
   (202) 547-0421

3. Washington DC 16th & K Street
   1612 K St NW Ste 100
   Washington, DC 20006-2802
   (202) 466-3777

4. Washington DC 2020 K Street
   2020 K Street W
   Washington, DC 20006-1806
   (202) 331-9572

5. Washington DC Catholic U
   204 Michigan Ave NE
   Washington, DC 20017-1005
   (202)232-7124

6. Washington DC Georgetown
   3329 M Street NW
   Washington, DC 20007-3514
   (202) 965-1414

7. Washington DC Chevy Chase

5225 Wisconsin Ave
Washington, DC 20015-2014
(202) 362-5003

8. Alexandria VA Old Towne
    685 N. Washington St
    Alexandria, VA 22314-1913
    (703) 739-0783

Set Lead 2:

PHILADELPHIA

AT PHILADELPHIA

Interview all employees of the following Kinko's stores and conduct logical investigation. Determine the ip address range allocated to the store for internet access, if not dynamically assigned. Determine the store's internet access and logging procedures. If LAMO is at any of the below listed locations, contact writer immediately.

Kinko's locations:

1. Philadelphia PA Marriott Conv Ctr
    1201 Market St
    Philadelphia, PA 19107-2817
    (215) 923-2520

2. Philadelphia PA Stock Exchng
    2001 Market St
    Philadelphia, PA 19103-7044
    (215) 561-5170

3. Philadelphia PA Spring Garden
    1816 Spring Garden St
    Philadelphia, PA 19130-3917
    (215) 567-2679

4. Philadelphia PA Univ City
    3923 Walnut St
    Philadelphia, PA 19104-3608
    (215) 386-5679

5. Philadelphia PA City Line
    4514 City Line Ave Fl 2
    Philadelphia, PA 19131-1509
    (215) 473-0500

6.   Philadelphia PA Northeast S/C
     9171 Roosevelt Blvd
     Philadelphia, PA 19114
     (215) 330-0212

Set Lead 3:

SAN FRANCISCO

AT SAN FRANCISCO

     Interview all employees of the following Kinko's stores and
conduct logical investigation. Determine the ip address range
allocated to the store for internet access, if not dynamically
assigned. Determine the store's internet access and logging
procedures. If LAMO is at any of the below listed locations,
contact writer immediately.

     Kinko's locations:

1.   San Franciso CA Nob Hill
     1800 Van Ness Ave
     San Francisco, CA 94109-3623
     (415) 292-2500

2.   San Francisco CA Pine Street
     369 Pine Street
     San Francisco, CA 94104-3302
     (415) 834-1053

3.   San Francisco, CA Mission District
     1965 & 1967 Market St
     San Francisco, CA 94103-1012
     (415) 252-0864

4.   San Francisco, CA Marina
     3225 Fillmore
     San Francisco, CA 94123-3402
     (415) 441-2995

5.   San Francisco, CA S of Market
     50 Fremont St
     San Francisco, CA 94105-2230
     (415) 512-7766

6.   San Francisco, CA South Beach
     303 2nd St
     San Francisco, CA 94107

b3 -2
b7E -3

(415) 495 8880

7.   San Francisco, CA Finance District
     201 Sacramento St
     San Francisco, CA 94111-3805
     (415) 834-0240

8.   San Francisco, CA Richmond District
     25 Stanyan Blvd
     San Francisco, CA 94118-3303
     (415) 750-1193

9.   San Francisco, CA Lakeshore
     1597 Sloat Blvd
     San Francisco, CA 94132-1222
     (415) 566-0572

◆◆

SecurityFocus ONLINE

qualys

Home | SFOnline | The Basics | Microsoft | Unix | IDS | Incidents | Virus

Columns   Mailing Lists   Library   [Search] [_____]   SFOnline ▽

NEWS

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-10-2010 BY [_____] UC BAW/DK/RYS

Lamo Bumped from NBC After Hacking Them

The helpful hacker demonstrates his techniques on camera for the NBC Nightly News, but lawyers kill the story when he cracks the broadcast network's own systems.
By **Kevin Poulsen**, Aug 27 2002 2:24PM

How did a mediagenic hacker like Adrian Lamo get himself bumped last week from a scheduled appearance on the NBC Nightly News with Tom Brokaw?

Perhaps with his impromptu on-camera intrusion into the peacock network's own computers.

The vagabond hacker known for his drifter lifestyle and his public forays into large and poorly-secured corporate intranets sat down at a Washington D.C. Kinko's laptop station earlier this month with a freelance NBC news producer to show-off his particular style of hacking -- the 21-year-old typically uses little more than an ordinary browser, possessing an eerie knack for finding undocumented Web servers and open proxies at large organizations.

That method has gotten Lamo deep into the electronic infrastructures of such companies as troubled telecom giant Worldcom, Internet portal Yahoo, and most recently the *New York Times*, where last February he exploited lax security to tap a database of 3,000 *Times* op-ed contributors, culling such tidbits of information as Robert Redford's social-security number, and former president Jimmy Carter's home phone number. But unlike most intruders, Lamo eventually goes public with his discoveries, and offers to help those he's hacked tighten their security *pro bono* -- an offer that's been accepted by several of his corporate targets. So far Lamo's managed to avoid prosecution, though federal officials in New York are believed to be investigating him for the *Times* hack.

> **'Maybe they should have just talked to the lawyers first. ... A little front end work to identify the pitfalls would have made it a good story.'**
> -- Journalism ethicist Kelly McBride

Lamo says NBC was taping him at Kinko's while he demonstrated security holes in a telecommunications company's systems, when the interviewer asked him if he'd be successful hacking NBC.

Five minutes and one guessed password later and Lamo was surfing the television network's private messaging system and an affiliate scheduling application that included internal memos and information on advertising rates.

Adrian Lamo does most of his hacking with an ordinary Web browser.

Screen shots of the hack provided by Lamo and reviewed by SecurityFocus Online include a page from an NBC vendor database with the network's trademark "living color" peacock and the warning, "All information contained on this Web site

b6 -1
b7C -1

they have to get it on the air, it's not the Pentagon Papers. ... A little front end work to identify the pitfalls would have made it a good story."

For his part, Lamo, who's not known for shrinking from controversy, charges the network with a failure of courage. "I can understand where they're coming from," says Lamo, in a telephone interview from somewhere on the East Coast. "But I like to think that in their place I'd take more of a risk."

<tips@securityfocus.com>

Discussion

Lamo Bumped from NBC After Hacking Them Not Really Anonymous
Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them phil
  Phil's and imbicile, and Lamo's a crim. Scott
    Phil's and imbicile, and Lamo's a crim. bollocks Damien
    Phil's and imbicile, and Lamo's a crim. NOT! Anonymous
    Phil's and imbicile, and Lamo's a crim. Ostracus
    Phil's and imbicile, and Lamo's a crim. Anonymous
    Phil's and imbicile, and Lamo's a crim. Anonymous
Lamo is a script kiddy Anonymous
  Lamo is a script kiddy Ira Wing
  Lamo is a script kiddy Anonymous
    Lamo is NOT a script kiddie Simon
    Lamo is a script kiddy Anonymous
    Lamo is a script kiddy Anonymous
    Lamo is a script kiddy Anonymous
  Lamo is a script kiddy kokorozashi
Lamo Bumped from NBC After Hacking Them Anonymous
  Lamo Bumped from NBC After Hacking Them Not Really Anonymous
    Lamo Bumped from NBC After Hacking Them Anonymous
    Lamo Bumped from NBC After Hacking Them Anonymous
      Lamo Bumped from NBC After Hacking Them Not Really Anonymous
  Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them Anonymous
  Lamo Bumped from NBC After Hacking Them Roger
  Lamo Bumped from NBC After Hacking Them Anonymous
  Lamo Jay
  Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them y2kprawn
Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them Anonymous
Lamo Bumped from NBC After Hacking Them Anonymous
Not Illegal! Anonymous
Lamo Bumped from NBC After Hacking Them MadLibs
My question is why ? Brian Gray // Bloodline
Lamo Bumped from NBC After Hacking Them M4rtin
Lamo Bumped from NBC After Hacking Them Ron
uhm..securityfocus is slow I am jack's name
So very smart Gleb
Lamo Bumped from NBC After Hacking Them Camel

[Post a comment]

Privacy Statement

kinkos com

Map Results

Here are the 5 Kinko's stores nearest you.

1. Kinko's - San Francisco CA Nob Hill

1800 Van Ness Ave
San Francisco, CA 94109-3623
Phone: (415) 292-2500
Fax: (415) 292-2504
EMail: usa0289@kinkos.com
Distance: 0.46 miles

Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - San Francisco CA Pine Street

369 Pine St
San Francisco, CA 94104-3302
Phone: (415) 834-1053
Fax: (415) 834-1054
EMail: usa0586@kinkos.com
Distance: 1.1 miles

Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - San Fran CA Mission District

1965 & 1967 Market St
San Francisco, CA 94103-1012
Phone: (415) 252-0864
Fax: (415) 252-0924

EMail: usa4095@kinkos.com
Distance: 1.2 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's - San Francisco CA Marina
3225 Fillmore
San Francisco, CA 94123-3402
Phone: (415) 441-2995
Fax: (415) 441-1381
EMail: usa5172@kinkos.com
Distance: 1.2 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's - San Francisco CA S of Market
50 Fremont St
San Francisco, CA 94105-2230
Phone: (415) 512-7766
Fax: (415) 512-7111
EMail: usa4099@kinkos.com
Distance: 1.3 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

Powered by Vicinity Corporation
US maps Copyright GDT, Inc. 2002. Contents Copyright © 2002 Vicinity Corporatio
All rights reserved. Terms of Use and Privacy Statement.

kinkos com

Map Results

Here are the 5 Kinko's stores nearest you.

@2001 Vicinity Corp. GDT

1. Kinko's - San Francisco CA South Beach
303 2nd St
San Francisco, CA 94107
Phone: (415) 495-8880
Fax: (415) 495-0300
EMail: usa0916@kinkos.com
Distance: 1.4 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - San Francisco CA Finance Dist
201 Sacramento St
San Francisco, CA 94111-3805
Phone: (415) 834-0240
Fax: (415) 834-0243
EMail: usa4096@kinkos.com
Distance: 1.4 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - San Francisco CA Richmond Dist
25 Stanyan Blvd
San Francisco, CA 94118-3303
Phone: (415) 750-1193
Fax: (415) 750-1199

EMail: usa5160@kinkos.com
Distance: 1.9 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's - San Francisco CA Lakeshore
1597 Sloat Blvd
San Francisco, CA 94132-1222
Phone: (415) 566-0572
Fax: (415) 566-3148
EMail: usa4094@kinkos.com
Distance: 5.1 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's - Sausalito CA Sausalito
2400 Bridgeway
Sausalito, CA 94965-1585
Phone: (415) 331-2093
Fax: (415) 331-2096
EMail: usa5167@kinkos.com
Distance: 6.6 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

Powered by Vicinity Corporation
US maps Copyright GDT, Inc. 2002. Contents Copyright © 2002 Vicinity Corporatio
All rights reserved. Terms of Use and Privacy Statement.

FBI(19-cv-1495)-1675

kinkos com

HOME | OUR SERVICES | LOCATIONS | SEA

Map Results

Here are the 5 Kinko's stores nearest you.

1. Kinko's - Philadelphia PA Marriott Conv Ctr
1201 Market St
Philadelphia, PA 19107-2817
Phone: (215) 923-2520
Fax: (215) 923-2360
EMail: usa0669@kinkos.com
Distance: 0.19 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - Philadelphia PA Stock Exchng
2001 Market St
Philadelphia, PA 19103-7044
Phone: (215) 561-5170
Fax: (215) 561-5346
EMail: usa0293@kinkos.com
Distance: 0.53 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - Philadelphia PA Spring Garden
1816 Spring Garden St
Philadelphia, PA 19130-3917
Phone: (215) 567-2679
Fax: (215) 567-2217

FBI(19-cv-1495)-1676

3/15/02

EMail: usa1217@kinkos.com
Distance: 0.84 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's - Philadelphia PA Univ City

3923 Walnut St
Philadelphia, PA 19104-3608
Phone: (215) 386-5679
Fax: (215) 386-3297
EMail: usa1210@kinkos.com
Distance: 2.0 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's - Philadelphia PA City Line

4514 City Line Ave Fl 2
Philadelphia, PA 19131-1509
Phone: (215) 473-0500
Fax: (215) 473-2903
EMail: usa1214@kinkos.com
Distance: 4.7 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

FBI(19-cv-1495)-1677

kinkos.com

HOME | OUR SERVICES | LOCATIONS | SEA

Map Results

Here are the 5 Kinko's stores nearest you.

1. Kinko's - Wynnewood PA Lancaster Avenue
292 E Lancaster Ave
Wynnewood, PA 19096-2126
Phone: (610) 896-2360
Fax: (610) 896-2431
EMail: usa0808@kinkos.com
Distance: 7.0 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - Cherry Hill NJ Kinko's Plaza Route 70
1160 Marlton Pike E
Cherry Hill, NJ 08034-2131
Phone: (856) 427-0099
Fax: (856) 427-0328
EMail: usa1220@kinkos.com
Distance: 9.2 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - Springfield PA Baltimore Pike
1001 Baltimore Pike
Springfield, PA 19064-2852
Phone: (610) 328-7877
Fax: (610) 328-9214

EMail: usa0284@kinkos.com
Distance: 9.8 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's - Philadelphia PA Northeast S/C
9171 Roosevelt Blvd
Philadelphia, PA 19114
Phone: (215) 330-0212
Fax: (215) 330-0375
EMail: usa0793@kinkos.com
Distance: 11.0 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's - Villanova PA Radnor
795 Lancastre Ave
Villanova, PA 19085-1517
Phone: (610) 527-0699
Fax: (610) 527-5153
EMail: usa0587@kinkos.com
Distance: 11.4 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

b6 -1
b7C -1

kinkos com

Map Results

Here are the 5 Kinko's stores nearest you.
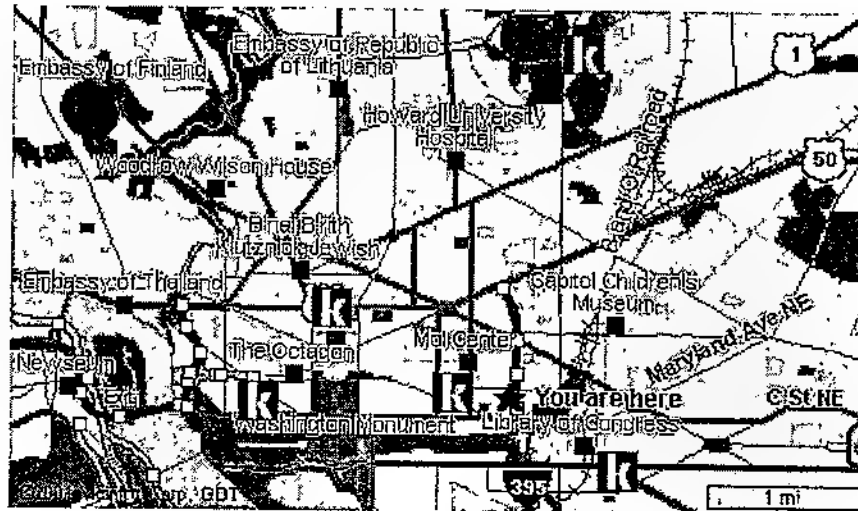
1. Kinko's - Washington DC 7th & D
325 7th St
Washington, DC 20004-2801
Phone: (202) 544-4796
Fax: (202) 347-8736
EMail: usa0671@kinkos.com
Distance: 0.37 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - Washington DC Capitol Hill
317 Pennsylvania Ave SE
Washington, DC 20003-1148
Phone: (202) 547-0421
Fax: (202) 543-8393
EMail: usa1810@kinkos.com
Distance: 0.86 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - Washington DC 16th & K Street
1612 K St NW Ste 100
Washington, DC 20006-2802
Phone: (202) 466-3777
Fax: (202) 466-4165

FBI(19-cv-1495)-1680

EMail: usa1822@kinkos.com
Distance: 1.3 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's - Washington DC 2020 K Street

2020 K St NW
Washington, DC 20006-1806
Phone: (202) 331-9572
Fax: (202) 331-9721
EMail: usa1815@kinkos.com
Distance: 1.7 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's - Washington DC Catholic U

204 Michigan Ave NE
Washington, DC 20017-1005
Phone: (202) 232-7124
Fax: (202) 232-3890
EMail: usa1805@kinkos.com
Distance: 2.3 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

Powered by Vicinity Corporation
US maps Copyright GDT, Inc. 2002. Contents Copyright © 2002 Vicinity Corporatio
All rights reserved. Terms of Use and Privacy Statement.

kinkos.com

[HOME][OUR SERVICES][LOCATIONS][SEA

Map Results

Here are the 5 Kinko's stores nearest you.

1. Kinko's - Washington DC Georgetown
3329 M St NW
Washington, DC 20007-3514
Phone: (202) 965-1414
Fax: (202) 333-7433
EMail: usa1801@kinkos.com
Distance: 2.9 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

2. Kinko's - Arlington VA Crystal City
1601C Crystal Square Arc
Arlington, VA 22202-3301
Phone: (703) 413-8011
Fax: (703) 413-8013
EMail: usa1828@kinkos.com
Distance: 3.0 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

3. Kinko's - Arlington VA Courthouse
2300 Clarendon Blvd
Arlington, VA 22201-3367
Phone: (703) 525-9224
Fax: (703) 525-4239

EMail: usa1820@kinkos.com
Distance: 3.9 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

4. Kinko's – Washington DC Chevy Chase
5225 Wisconsin Ave
Washington, DC 20015-2014
Phone: (202) 362-5003
Fax: (202) 362-5163
EMail: usa0388@kinkos.com
Distance: 5.8 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

5. Kinko's – Alexandria VA Old Towne
685 N Washington St
Alexandria, VA 22314-1913
Phone: (703) 739-0783
Fax: (703) 739-0785
EMail: usa1819@kinkos.com
Distance: 5.9 miles
Driving Directions | Location Map | Order Online with Print to Kinko's
(Store pick up available)

GTK:gtk

b3 -2
bo -1
b7C -1
b7E -3

1

On 09/19/2002, the following investigation was conducted by Special Agent [ ] and Special Agent [ ] of the Washington Field Office, regarding ADRIAN LAMO:

bc 1,5
b7C 1,5

[ ] (Philadelphia, D.C., and Baltimore), Kinko's Inc. Corporate Offices, 1033 Easton Road, Willow Grove, Pennsylvania 19090, telephone number [ ] facsimile number (610) 631-8999, e-mail address [ ] was contacted at the Kinko's store located at 325 7th Street, N.W., Washington, D.C. 20004-2801, telephone number [ ]. Also present during the investigation was [ ] Kinko's Inc. 3232A Crain Highway, Waldorf, Maryland 20603-4849, telephone number [ ] extension [ ] cell phone number [ ] [ ] e-mail [ ]

[ ] was advised by the investigating Agents that the FBI was seeking the cooperation of Kinko's representatives in the Washington, D.C. metropolitan area regarding a criminal investigation. He was also advised that the subject of this investigation may be using internet portals at Kinko's stores in the Washington, D.C. area, among others, to launch computer intrusions against major corporations.

[ ] and [ ] advised that they would cooperate with the FBI in anyway that they could. [ ] will provide the investigating Agents with the IP addresses for all of the Kinko's stores in the Washington, D.C. area. [ ] will notify all of the Washington, D.C. area store managers and advise them to cooperate with the FBI during this investigation.

bo 5,
b7C 5

SERIALIZED

NOV 2 0 2002

b3 -2
b7E -3

wpd

UPLOADED
WITH/TEXT ✓
WITH/OUT TEXT
BY
DATE 9-24-02

SERIAL

OCT · 0 2002

b3 -2
b6 -1,
b7C -1,5
b7E -3

FD-302 (Rev 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

b6 -1,6
b7C -1,6

Date of transcription   09/20/2002

email [   ] Kinko's, telephone number [   ] was telephonically contacted by the interviewing agent. After being advised as to the identity of the interviewing agent and the purpose of the interview, [   ] provided the following information:

b7E -1

Investigation on   09/19/2002   at   New York, NY   (telephonically) b6 -1
                                                                                          b7C -1
File #[   ]   Date dictated   09/20/2002   b3 -2
by   SA [   ]   b7E -3

email Kin.wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 13-13-2010 BY [ ] UC BAW/DK/RIS

OCT 0 1 2002

b3 -2
b6 -1
b7C -1
b7E -3

10/01/2002
CAH:cah

    The attached email was sent to [_____] Kinko's, regarding preserving the video tapes from their Washington, DC stores for the dates of August 25/26, 2002 due to the hack of NBC by ADRIAN LAMO from one of their Washington, DC stores   Writer is still attempting to determine which Kinko's he utlized to commit the intrusion

FBI(19 cv 1495) 1688

b3   2
b7E 5

To[_____]

Subject: Adrian Lamo

Hi,[_____]

Thanks for the information the other day. I am still waiting to receive some more information regarding IP addresses and text strings that should help in the search you are doing for us. I will forward them onto you as soon as I get them.

Another issue came up and I was wondering who to address it to, as you know on August 25/26, LAMO hacked into a telecommunications company and then into NBC while being filmed by a news team. He did all of his hacking from a Kinko's in DC. I am still investigating which store in DC he was in but until then can we have the video tapes from all the stores in DC preserved. I know you usually hold them for 60 days and I am hoping to have the right store by then but just in case I don't can they be preserved for more than 60 days? Do you need anything from me to preserve the tapes? Or if I subpoena the tapes could they be sent to me? I believe there are approximately 12 stores in the DC area or are there more?

I appreciate all of your help in this matter.

Sincerely,

[_____]

phonel.wpd

UPLOADED

WITH/TEXT _____ ✓

WITH/OUTTEXT _____

BY _____

DATE 10-2-02
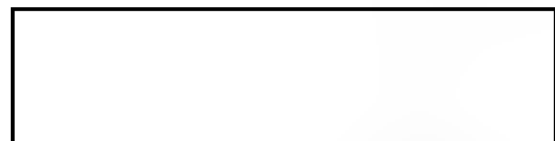
10/01/2002
CAH:cah

b3   2
b6   1
b7C   1
b7E   5

An ACS check was conducted into the following names. The names were obtained through subscriber records for telephone calls placed to them by ADRIAN LAMO.

1. [ ]
   billing address: [ ]
   service address: [ ]
   SSN [ ]
   DL: [ ]
   employer: [ ]
   telephone number: [ ]

b6   5
b7C   5
b7E   2

2. [ ]
   billing address [ ]
   SSN [ ]
   employer: [ ]
   telephone number: [ ]

3. [ ]
   [ ]
   billing address: [ ]
   CBR: [ ]
   telephone number [ ]

4. SEAMS LIKE OLDE TIMES [ ]
   [ ]
   billing address: [ ]
   CBR: [ ]
   telephone number: [ ]

b6   5
b7C   5
b7E   2

5. [ ]
   billing address [ ]
   DL: [ ]
   SSN [ ]
   employer: [ ]
   CBR. [ ]
   telephone number: [ ]

6. UNIVERSITY OF REDLANDS [ ]

b3 -2
b7E -3

billing address: 1200 E. Colton AVenue, Redlands, CA 9234-3720
telephone number: (909) 307-7558

7   MICROSOFT CORPORATION
        3635 157th Avenue NE
        Redmond, WA 98052-5326
        CBR: (425) 882-8080
        telephone number   (425) 936-7751

} /E   ∠

sub2.wpd

UPLOADED

WITH/TEXT ✓

WITH/OUT TEXT

BY

DATE 10-8-02

Subfile opened 10-8-02

SEARCHED ___ INDEXED ___
SERIALIZED ___ FILED ___

OCT 0 4 2002

FBI — N.

L6   1
b/C   1
b3
b/E   3

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/04/2002

To: New York

From: New York
       Squad C-37
       Contact: SA [_____]

Approved By: [_____]

Drafted By: [_____] :slf

Case ID #: [_____]

b6   6
b6   1
b7C   1
b7E   3

Title: LAMO, ADRIAN
        New York Times-Victim;
        Computer Intrusion;
        OO:NY

Synopsis: Request to open sub-files and change of title.

Details: Writer requests the following sub-files to be opened in above referenced case:

Also, please open the following Sub files:

    Sub B   [_____]

♦♦   b6   4

18 2002

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-13-2010 BY [ ] UC BAW DH/KJS

b6 -1
b7C -1

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   09/25/2002

[ ] date of birth [ ] social security account number [ ] was interviewed at his place of employment, Kinko's, 325 7th Street, N.W., Washington, D.C. 20004. After being advised of the identity of the interviewing Agent and the purpose of the interview, [ ] provided the following information:

He is a [ ] for Kinko's. His normal shift is [ ] is the [ ]

b6 -5,6
b7C -5,6

[ ] was shown a photograph of ADRIAN LAMO by the interviewing Agent. He recognized LAMO as a Kinko's customer. He recalls assisting LAMO at this Kinko's location approximately three or four months ago.

Between approximately 2:00 pm and 3:00 pm one afternoon, LAMO entered the aforementioned Kinko's to fax a document. There was a store assistant helping another customer with a fax and LAMO became impatient. LAMO approached [ ] and asked if there was another fax machine that he could use. [ ] said that there was another machine and that he would assist him.

While assisting LAMO, [ ] engaged him in a short conversation. LAMO stated that he was trying to fax a document to resolve a situation whereby his laptop computer had been confiscated.

b6 -6
b7C -6

LAMO claimed that a friend borrowed his laptop and used it to web surf child pornography sites. He was sitting next to said friend at a library when his laptop was confiscated. LAMO was not specific as to who confiscated it.

[ ] described LAMO as follows:

Sex: Male
Race: White
Age: Early 20's
Height: 5'11" (approximately)

b3   2
b6   1
b7   1
b7E   5

Investigation on	09/20/2002	at	Washington, D.C.
File #			Date dictated N/A
by SA			

FBI(19-cv-1495)-1696

```
Weight:              165
Build:               Thin                              b6  -6
Hair:                Brown                             b7C -6
Hair style:          Short                             b3  -2
Eyes:                Green                             b7E -3
Facial hair:         None
Misc:                Well groomed
Clothing:            T-shirt and jeans
```

[   ] remembered LAMO because of his engaging green eyes and the unusual conversation about the laptop.

GTK:gtk

b3 -2
bo -1
b7C -1
b7E -3

      The following investigation was conducted on 09/20/2002 by Special Agent (SA) [   ] regarding ADRIAN LAMO:

      The investigating Agent contacted employees of the Kinko's store located at 325 7th Street, N.W., Washington, D.C. 20004. Store employees were shown a picture of ADRIAN LAMO. [   ] was the only employee who recognized LAMO. His comments are submitted to this file under separate cover.

b6 -1,6
b7C -1,6

      The following is a list of the Kinko's employees that were contacted at this location:

Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service

b6 -5
b7C -5

b3 -2
bo -1
b7C -1
b7E -3

FBI(19-cv-1495)-1698

GK268022.IN

UPLOADED
WITH/TEXT_____ ✓
WITHOUT TEXT_____
BY____(W)____
DATE __10-10-02__

b3 -1,2
b6 -1
b7C -1
b7E -3

CAH:cah
10/09/2002

    Writer telephonically contacted [   ] telephone number [   ] in response to a message left by [   ] pertaining to a subpoena [   ] The subpoena requested [   ]
[   ] ADRIAN LAMO.

    [   ] explained that for the time period requested,
[   ] stated that there were [   ] [   ] would organize the requested information and would provide it to the writer in a timely manner.

wpd

OCT 1 0 2002

FBI —

SERIALIZED

b3   2
b6   1,c
b7C   1,6
b7E

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/26/2002

[blacked out] Information Security,
9443 Springboro Pike, Miamisburg, OH 45342, email: b6   6
[blacked out] telephone number [blacked out] and   b7C   6
facsimile number [blacked out] was interviewed at 26 Federal
Plaza, New York, NY. After being advised as to the identities of
the interviewing agents and the purpose of the interview, [blacked out]
provided the following information:

[blacked out] is the [blacked out] of Information Security
for LEXIS-NEXUS. [blacked out] became involved in the investigation of
the computer intrusion of ADRIAN LAMO into the NEW YORK TIMES and
then LEXIS-NEXUS in May 2002.

Referring to the log files of the unauthorized access
by ADRIAN LAMO into LEXIS-NEXUS, [blacked out] stated that the log files
are [blacked out]

b6   6
b7C   6
b7E   1

[blacked out] LAMO gained unauthorized access to this
intranet page and he created the userids TOOMANYSECRETS,
PROTAGONIST, LOCUSTS, VAISHNAV and NUIUJB. [blacked out]
[blacked out] [blacked out] verified with the TIMES that these
userid's were not created or utilized by any employee of the
TIMES.

After the userids were created [blacked out]
[blacked out]
[blacked out] explained that [blacked out]
[blacked out]
[blacked out] [blacked out] was able to determine that some of the userids   b6   6
were access from KINKOS. The userids created by LAMO conducted   b7C   6
approximately 2700-3000 searches on LEXIS-NEXUS. Searches   b7E   1
ranging from name, address, social security number, detailed
motor vehicle records, news libraries, etc were conducted.
[blacked out] stated that the number of searches conducted by the

Investigation on 07/25/2002   at New York, NY   b6   1
                                                                        b7C   1
File # [blacked out]   Date dictated   b7E   ...
        SA [blacked out]
by   SA [blacked out]   :slf(_)   b7E   ...

FBI(19 cv 1495) 1/02

Continuation of FD-302 of _____ , On 07/25/2002 , Page 2

userids were much greater than the normal activity of the TIMES'   b6   ᵒ
users. The number of searches performed by the TIMES' account   b/C   6
greatly increased once the userids were created. [   ]was able   Ł ⁵   ⁻
to determine that the increase in the TIMES' usage of their   b/E   ₃
services was caused by the userids TOOMANYSECRETS, PROTAGONIST,
LOCUSTS, VAISHNAV and NUIUJB. The cost of the amount of services
utilized by the five (5) userids was approximately $300,000. The
TIMES was originally charged for this activity. At this time,
[   ]is unaware of whether or not the $300,000 has been
refunded to the TIMES by LEXIS-NEXUS. Because of the
unauthorized access by LAMO, LEXIS-NEXUS has suffered a monetary
loss.

          Log files are maintained by LEXIS-NEXUS in relation to
the all userid's activity. The original log files pertaining to
the userid's created by LAMO have been secured.

Lexis.wpd

OCT 1 0 2002

FBI — NEW YORK

b3 -2
bC -1
b7C -1
b7E -3

CAH:cah
07/10/2002

bo   1,6
b7C 1, c
b3   2
b7E 3

[   ] Information Security, 9443
Springboro Pike, Miamisburg, OH 45342, email:
[   ] telephone number [   ] and
facsimile number [   ] contacted the writer by encrypted
email. [   ] sent the writer the appropriate log files
pertaining to the unauthorized use by ADRIAN LAMO into LEXIS-
NEXUS.

The log files will be maintained in the file.

wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE ___ 10 ___ U ___ RAS

b3 -2
b6 -1,6
b7C -1,6
b7E -3

FD-302 (Rev. 10-6-95)

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/10/2002

[   ] KINKO's, Legal Department, telephone
number [   ] was
telephonically contacted by the interviewing agent. After being
advised as to the identity of the interviewing agent and the
purpose of the interview, [   ] provided the following
information:

b6   6
b7C   6

[   ] is a member of KINKO's Legal Department. [   ]
stated that with a subpoena KINKO's would be able to provide the
Internet Protocol (IP) address ranges for their stores in
Washington, DC, Philadelphia, PA and San Francisco, CA. [   ]
stated that once the subpoena was received she would forward it
to [   ] who is familiar with the investigation.

Investigation on 10/09/2002 at New York, NY   (telephonically)

b3 -2
b6 -1
b7C -1
b7E -3

File # [   ]   Date dictated 10/10/2002

by SA [   ]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency;
it and its contents are not to be distributed outside your agency.

FBI(19 cv 1495) 1/0/

nbcnewmm.wpd

UPLOADED

WITH/TEXT ✓

WITHOUT TEXT

BY

DATE 10-11-02

SERIALIZED___ FILED___

OCT 0 9 2002

b
bo   1
b7C   1
b7E   3

10/19/2002
CAH:cah

b3   2
b6   1, ░
b/C   1, ░
b/E   ░

          The attached email was received by [   ] Microsoft, email address: [   ] in reply to an email sent to him by writer. [   ] stated that the phone number [   ] belongs to [   ] for MSNBC. That number was called by ADRIAN LAMO on eight (8) occassions.

b3 -2
b7E -3

phones.wpd

UPLOADED
WITH TE
WI
BY
DATE 10-18-02

b3 -2
b6 -1
b7C -1
b7E -3

10/15/2002
CAH.cah

b3 -2
bo -1
b7C -1
b7E -2,3

An ACS and [   ] checks were conducted into the following names   The names were obtained through subscriber records for telephone calls placed to them by ADRIAN LAMO

1. [   ]
   Alias: [   ]
   address: [   ]
   telephone: [   ]
   telephone: [   ]
   home telephone: [   ]
   business telephone: [   ]
   SSN: [   ]
   DOB: [   ]
   Employer: [   ]

2. [   ]
   address: [   ]
   other address: [   ]
   telephone: [   ]
   SSN: [   ]
   DOB [   ]
   Sex: Female

3. [   ]
   address [   ]
   telephone: [   ]
   home telephone: [   ]
   work telephone: [   ]
   SSN: [   ]

4. [   ]
   address: [   ]
   telephone: [   ]
   home telephone: [   ]
   work telephone: [   ]
   SSN: [   ]
   DOB: [   ]

5. [   ]
   address [   ]
   other address: [   ]

bo -5
b7C -5

FBI(19-cv-1495)-1715

b3 -2
b7E -3

telephone [ ]
SSN: [ ]
DOB. [ ]

6. [ ]
   address: [ ]
   telephone: [ ]
   home telephone [ ]
   work telephone: [ ]
   SSN: [ ]

7. [ ]
   address [ ]
   telephone. [ ]
   home telephone: [ ]
   work telephone: [ ]
   SSN [ ]
   DOB [ ]

8. [ ]
   employer [ ]
   address [ ]
   other address: [ ]
   telephone: [ ]
   home telephone: [ ]
   telephone [ ]
   SSN: [ ]
   DOB [ ]

9. [ ]
   address: [ ]
   other address [ ]
   telephone: [ ]
   SSN(ELLIE): [ ]
   DOB(ELLIE) [ ]
   other people at address: [ ] and [ ]
   DOB: [ ]

10. [ ]
    address [ ]
    home telephone [ ]
    telephone: [ ]
    Employer: [ ]

b6 -5
b7C -5

11. [ ]

Aliases: [ ]
address: [ ]
telephone: [ ]
home telephone: [ ]
work telephone [ ]
SSN: [ ]
DOB: [ ]
Employer: [ ]

12 [ ]

Alias: [ ]
address: [ ]
other address. [ ]
telephone: [ ]
SSN: [ ]
DOB: [ ]

13. [ ]

address: [ ]
telephone: [ ]
home telephone: [ ]
work telephone. [ ]
Employer: [ ]
SSN: [ ]
DOB: [ ]

address

b6
b7C

BAB:bab

1

be
b7C
b3
b7E

The following investigation was conducted on 10/09/2002
by Special Agent (SA) [_____] regarding ADRIAN LAMO:

The investigating Agent contacted employees of the
Kinko's store located at 204 Michigan Avenue, N.E., Washington,
D.C. 20017. Store employees had a picture of ADRIAN LAMO posted
prominently in their work space. All of the employees had
previously been briefed on LAMO, and none had ever seen him
before.

This location has one (1) "Design" station and four (4)
work stations available for public use as well as 2 Apple
computers. They do not permit users to connect their own
machines to the Kinko's network, and they do not have a laptop
docking-station currently available. [_____]
[_____] expects that a laptop docking-station will be available
soon.

[_____]
[_____] The subnet for
the workstations in the store appears, from viewing a workstation
configuration, to be [_____] [_____] the most
technically aware employee, was not familiar with the access
procedures, firewall, or computer logging done locally at the
Michigan Avenue Kinko's.

b7E -1
b6 -5
b7C -5

The hours for this location are:

Weekdays - 7 a.m. to 9 p.m.
Saturday - 9 a.m. to 5 p.m.
Sundays - Closed

The following is a list of the Kinko's employees that
were contacted at this location:

b3 2
b6 5
b7C 5
b7E 5

Customer Service
Customer Service
Customer Service

NOV 0 2002
FBI

FBI(19-cv-1495)-1718

nbc.wpd

UPLOADED

WITH/TEXT ✓

WITHOUT TEXT

BY

DATE 10-23-02

b3 -2
b6 -1
b7C -1
b7E -3

b3   6
b6   1
b7C   1
b7E   3

CAH:cah
10/09/2002

[ ]   Writer was telephonically contacted by [ ]
[ ]   Legal Department, telephone number [ ] Upon
the request of AUSA [ ]   writer explained that she was
verbally requesting [ ]
[ ] pertaining to the computer intrusion of ADRIAN LAMO.
Writer informed [ ] that they were currently in the   b6   4,5
process of obtaining Department of Justice (DOJ) approval for a   b7C   4,5
subpoena requesting the logs from [ ] stated that
she was not sure if DOJ approval was needed to obtain the
technical logs. She further stated that all that may be needed
is a Grand Jury subpoena but she would have to verify this with
others in their Legal Department. [ ] said that if any
part of the LAMO story was to be subpoenaed then DOJ approval
would be necessary.

       [ ] informed writer that she would get back to her
regarding this matter.

b3 -2
b7E -3

FBI(19 cv 1495) 1/20

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE _____ BY _____

b3 2
b6 1
b7C 1
b7E 3

1

The following investigation was conducted by
SA [   ] and SA [   ] at San Francisco,
California on October 16, 2002:

[   ] born [   ] at
KINKO'S, 1597 Sloat Boulevard, San Francisco, California (CA)
94132, telephone number [   ] after being shown a picture
of ADRIAN LAMO, did not recognize LAMO as ever using that KINKO'S
facility. None of the other employees present recognized LAMO.

b6 1,5
b7C 1,5

[   ] born [   ] at
KINKO'S, 303 2nd Street, San Francisco, CA 94107, telephone
number [   ], after being shown a picture of ADRIAN LAMO,
did not recognize LAMO as ever using that KINKO'S facility. None
of the other employees present recognized LAMO.

[   ] born [   ] at KINKO'S,
25 Stanyan Boulevard, San Francisco, CA 94118, telephone number
[   ], after being shown a picture of ADRIAN LAMO, did not
recognize LAMO as ever using that KINKO'S facility. None of the
other employees present recognized LAMO.

[   ] born [   ] at
KINKO'S, 3225 Fillmore, San Francisco, CA 94123, telephone number
[   ] after being shown a picture of ADRIAN LAMO, did not
recognize LAMO as ever using that KINKO'S facility. None of the
other employees present recognized LAMO.

[   ] born [   ] at KINKO'S,
1800 Van Ness Avenue, San Francisco, CA 94109, telephone number
[   ], after being shown a picture of ADRIAN LAMO, did not
recognize LAMO as ever using that KINKO'S facility. None of the
other employees present recognized LAMO.

b6 -5
b7C -5

[   ] born [   ] at
KINKO'S, 369 Pine Street, San Francisco, CA 94104, telephone
number [   ] after being shown a picture of ADRIAN LAMO,
did not recognize LAMO as ever using that KINKO'S facility. None
of the other employees present recognized LAMO.

[   ] born [   ] at KINKO'S,
201 Sacramento Street, San Francisco, CA 94111, telephone number
[   ] after being shown a picture of ADRIAN LAMO, did not
recognize LAMO as ever using that KINKO'S facility. None of the
other employees present recognized LAMO.

b3 2
b7E 3

b3 2
b7E

[_____] born [_____] at
KINKO'S, 50 Fremont Street, San Francisco, CA 94105, telephone
number [_____] after being shown a picture of ADRIAN LAMO,
did not recognize LAMO as ever using that KINKO'S facility. [____]
[____] born [_____] employee at this KINKO'S site, thought
that LAMO seemed familiar as someone who may have used the
computer facility two to three weeks ago. [_____] could not confirm
that it was LAMO. None of the other employees present recognized
LAMO.

b6 -5
b7C -5

[_____] born [_____] at KINKO'S,
1965 Market Street, San Francisco, CA 94103, telephone number
[_____] after being shown a picture of ADRIAN LAMO, did not
recognize LAMO as ever using that KINKO'S facility. None of the
other employees present recognized LAMO.

        KINKO'S Internet customers can bypass the employee
counter and go directly to the Internet stations and pay without
having to log any information. Any customer can insert a prepaid
or credit card to begin Internet service. The KINKO'S employees
present did not know which Internet Protocol (IP) addresses were
assigned to the customer Internet stations, nor did they know the
method by which each IP address is assigned to each station.

        A flyer of LAMO was left at each KINKO'S to circulate
and post in a private location to verify with the rest of the
employees whether or not any of them had recognized LAMO. The
flyer instructs the KINKO'S employees to contact SA [____] or SA
[_____] if they see LAMO. In addition, the employees were
instructed to note the location and time LAMO used the computer
facility. The flyer is attached hereto and made a part of the
case file.

b6 1
b7C 1

(Rev. 08-28/2000)

bo -1
b7 -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 10/28/2002

To: New York   Attn: [   ]

From: San Francisco
       Squad 14B/Hayward RA
       Contact: [   ]

Approved By: [   ]

Drafted By: [   ]:sh

Case ID #: [   ]

Title: ADRIAN LAMO;
        New York Times-Victim;
        Computer Intrusion;
        OO:NY

b3 -2
bo -1
b7C -1
b7E -3

Synopsis: To report the completion of the San Francisco Lead.

Reference: [   ]

Administrative: Case agent [   ] was contacted
regarding the [   ] used by KINKO'S in the
San Francisco area. [   ] noted that KINKO'S had been
[   ]

b3 -2
b6 -1
b7C -1

Enclosure(s): Original and two copies of the insert, flyer of
ADRIAN LAMO, and 1-A of original notes.

Details: On October 16, 2002, SAs [   ] and [   ]
[   ] conducted an investigation at all the KINKO'S sites
in San Francisco. All employees present were shown a flyer of
ADRIAN LAMO and asked whether he was ever seen using the customer
Internet stations. None of the KINKO'S employees could confirm
ever seeing LAMO. The flyer was left at each site along with
contact information.

b6 -1
b7C -1

       KINKO'S Internet customers can bypass the employee
counter and go directly to the Internet stations and pay without
having to log any information. Any customer can insert a prepaid
or credit card to begin Internet service. The KINKO'S employees
present did not know which Internet Protocol (IP) addresses were
assigned to the customer Internet stations. In addition, the
method by which each IP address is assig[   ]
Internet station is unknown.

b3 -2
b7E -3

SERIALIZED
NOV 0 2002

FBI(19-cv-1495)-1723

b3 -2
b7E -3

San Francisco considers this lead covered.

♦♦

JTC:jtq

b3 -2
b6 -1, 5
b7C -1,5
b7E -3

1

The following investigation was conducted by Special
Agent (SA) [   ] at Alexandria, Virginia, on
10/24/2002:

With the cooperation of Kinko's [   ]
[   ] all employees of the Kinko's store located at 685 N.
Washington Street, Alexandria, Virginia, 22314, telephone number:
[   ] were shown a photograph of ADRIAN LAMO. Store
employees were asked to determine if they recalled the presence
of LAMO, or anyone who matched the description of LAMO, at the
Kinko's store in the past. These queries met with negative
results.

The following is a list of the Kinko's employees that
were contacted at this location:
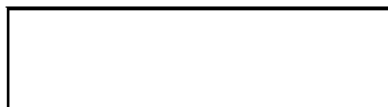
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service
Customer Service

b6 -5
b7C -5

Wanted for Questioning

Date: **10/16/2002**

Case #:

Name: **Adrian Lamo**

Address:

San Francisco, CA 94102

Sex: **M**

Eyes: **Green**

Hair: **Brown**

Race: **White**
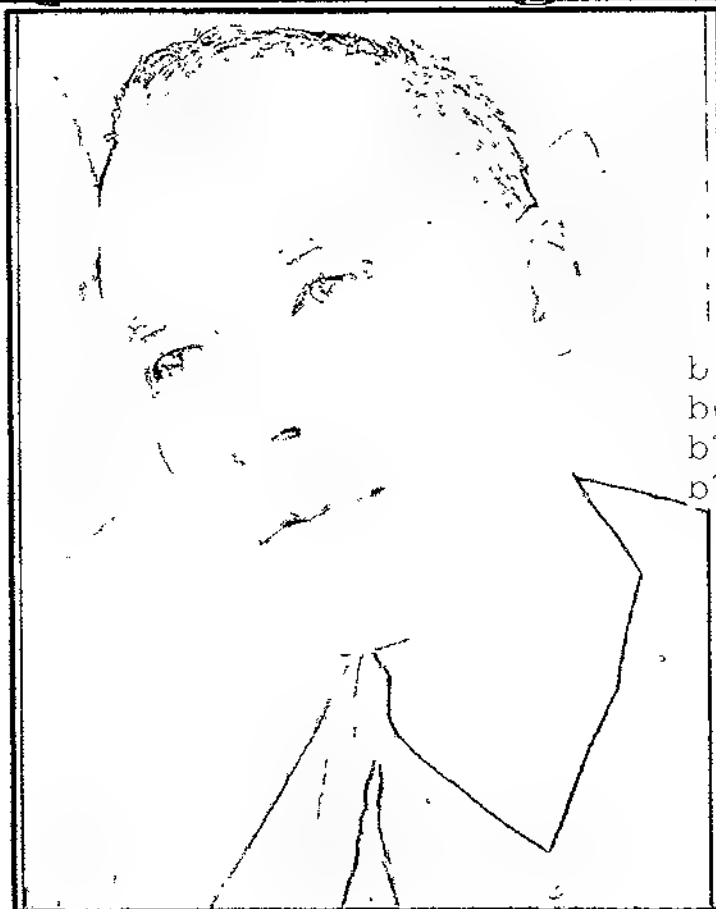
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2 13 __ BY ___

b3 -2
b6 -1
b7C -1
b7E -3

OTHER INFORMATION BELOW

Adrian Lamo is under investigation by NY FBI for numerous computer intrusions. Currently, there is no warrant for his arrest. It is believed that Lamo frequents Kinko's Copy Centers in the San Francisco area to log into the Internet. If Lamo is located, contact San Francisco FBI at the phone number listed below.

FBI SA _____ or SA _____

or (415) 553-7400 (24 hours)

b6   1
b7C 1

TRAK (356:1.6.48)

- sent due to request
by [   ]

SERIALIZED

OCT 1 5 2002

b3 -1,2
b6 -1
b7 -1
b7E -3

b6   1,5
b7C   1,5
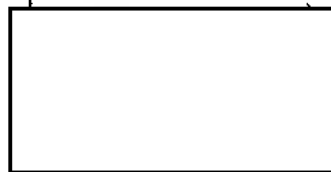
[ ] 03:58 PM 10/10/02 -0700, Verification of compliance with subpoe

To: [ ]
From: SA [ ]
Subject: Verification of compliance with subpoena
Cc:
Bcc:
Attached:

Hi, [ ]

Thank you for your compliance with the subpoena [ ] requesting the [ ]
[ ] By receiving the facsimile from your office
dated 10/10/2002, you are now in compliance with the subpoena. Personal appearance is not
required as the facsimile satisfies the subpoena.

b6 -1,5
b7C -1,5
b3 -1

If you have any questions I can be contacted at [ ]

Thank you,
SA [ ]

b6 1,5
b7C 1

lexisz.wpd

SERIALIZED FILED

NOV 1 2 2002

b3 -2
bo -1
b7C -1
b7E -3

CAH:cah
11/12/2002

b3 -2
b6 -1
b7C -1
b7E -1, 3
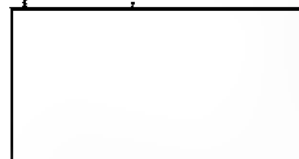
    SA [ ] received a CD Rom in the mail from [ ] The CD Rom
contains the [ ] by
ADRIAN LAMO

    A copy will be maintained in the file.

(Rev. 08-28-2000)

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 11/18/2002

To: New York   Attn: Squad C-37

From: Washington Field
      CR-16/NVRA
      Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ] gtk

Case ID #: [   ]

Title: ADRIAN LAMO;
       NEW YORK TIMES-VICTIM;
       COMPUTER INTRUSION;
       OO:NY

b3 -2
b6 -1
b7C -1
b7E -3

Synopsis: To report results of WFO investigation and to close
lead.

Reference: [   ]

Details: As per request, WFO conducted investigations at the
following Kinko's locations in the Washington, D.C. area:

1. 325 7th Street, NW
    Washington, D.C. 20004-2801
    (202) 544-4796

2. 317 Pennsylvania Avenue, SE
    Washington, DC 20003-1148
    (202) 547-0421

3. 1612 K Street, NW, Suite 100
    Washington, DC 2000~-2802
    (202) 466-3777

4. 2020 K Street, NW
    Washington, DC 20006-1806
    (202) 331 9572

5. 204 Michigan Avenue, NW
    Washington, DC 20017-1005
    (202) 232-7124

SERIALIZED
NOV 20 2002

b3
b7E -3

6.   3329 M Street, NW
     Washington, DC 20007-3514
     (202) 965-1414

7.   5225 Wisconsin Avenue, NW
     Washington, DC 20015-2014
     (202) 362-5003

8.   685 N. Washington Street
     Alexandria, .VA 22314-1913
     (703) 739-0783.

All employees at the aforementioned Kinko's locations
were shown a picture of ADRIAN LAMO and asked if they had any
knowledge of him or had seen him in their respective Kinko's
store. With one exception, of which was previously reported,
none of the Kinko's employees had seen or had knowledge of ADRIAN
LAMO.

Pictures on LAMO were left at each Kinko's location and
have been posted in the employees break areas. SA [   ]
contact information was also provided to the employees along with
instructions to contact him immediately if LAMO was seen.

b(-1
b7(-1

Per a previous telephone conversation between SA [   ]
and SA [   ] arrangements have been made for NYO to
obtain store specific Internet Protocol addresses by means other
than WFO investigators.

Original FD-302s and inserts pertaining to WFO
investigations at each of the aforementioned Kinko's locations
have been sent under separate cover to the NYO.

WFO considers this lead covered and closed.

2

LEAD(s):

Set Lead 1:

NEW YORK

AT NEW YORK

Read and Clear.

♦♦

3

b6   1
b/C   1
b3   2
b/E   3

KRM:krm

1

On 11/14/2002, Special Agent _____
Washington Field, conducted logical investigation with reference
to the above case number, _____ SA _____ met with _____
_____ for Kinko's Copy Service   b6   1,5
in the Washington, D.C. area. SA _____ and _____ met at the   b/C   1,5
Kinko's Center at 5225 Wisconsin Ave., Washington, D.C. 20015-   b3   2
2014. SA _____ told _____ that the Bureau needed to determine   b7E   3
the IP address range allocated to and internet access and logging
procedures for the below listed Kinko's Copy Centers.
Additionally, SA _____ provided a recent picture of the subject
of referenced investigation, ADRIAN LAMO.

          _____ was very cooperative and advised that all
Kinko's Copy Centers in the Washington Metropolitan area,
including the below listed, had current pictures of LAMO posted
in the employee's break rooms. Also, _____ had personally   b6   -5
spoken with all managers at Washington area stores and relayed   b7C -5
the above requests from the Bureau to them. Managers of
individual Kinko Stores queried all employees at their respective
locations to determine if anyone had ever seen LAMO at the store.
With regard to the below stores, no employees had seen LAMO.

Kinko's Copy Center Locations

Washington DC Capital Hill   Washington DC 16th & K St.
317 Pennsylvania Ave., SE   1612 K St., NW, Ste. 100
Washington, D.C. 2003-1148   Washington, D.C. 20006-2802

Washington DC 2020 K St.   Washington DC Georgetown
2020 K St., NW   3329 M St., NW
Washington, D.C. 200065-1806   Washington, D.C. 20007-3514

Washington DC Chevy Chase
5225 Wisconsin Ave.
Washington, D.C. 20015-2014

b3   2
b6   1
b/C   1
b/E   3

MAR 1 9 2003
FBI - NEW YORK

FBI(19-cv-1495)-1734

krm 31901.ins

FD-302 (Rev. 10-6-95)

bo   1
b7C   1

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   11/06/2002

     Source, who is not in a position to testify, provided the following information:

     Source was contacted regarding a lead from the New York Division on case number [_____] requesting that Sources be canvassed regarding any information about subject Adrian Lamo and his possible involvement in several computer intrusions.

    b3 -2
    b7E -3

     Source advised that he/she did not have any information on Lamo, and has not seen this type of intrusion on his/her network.

     The lead from New York Division is attached to and made part of this FD-302.

FILED
DEC 1 0 2002
NEW YORK

b3 -2
b6 -1
b7C -1
b7D -1,2
b7E -3
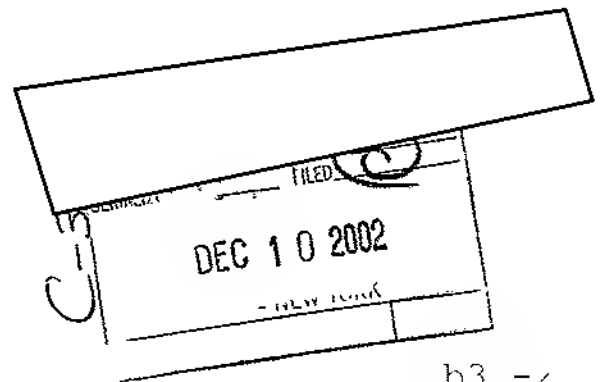
Investigation on   05/31/02   at [_____]

File # [_____]   Date dictated   11/06/02

by   SA [_____]

FBI(19 cv 1495) 1/35

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Precedence: ROUTINE   Date: 03/14/2002

To: All Field Offices   Attn: NIPC SSA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-_-2_ BY [ ] TC BAW/TC/B/S

From: New York
      Squad C-37
      Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ]slf

Case ID #: [   ]

b5   2
b6   1
b7C   1
b7E   5

Title: ADRIAN LAMO;
      New York Times-Victim;
      Computer Intrusion;
      OO:NY

Synopsis: Canvass all FBI Offices for positive information regarding ADRIAN LAMO.

Details: In February 2002, LAMO discovered several misconfigured proxy servers acting as doorways between the public Internet and the New York Times' private intranet. LAMO utilized the proxy servers to gain access to the New York Times network. Once on the network, LAMO cracked a password for a userid with supervisor rights. Utilizing this userid he was able to broaden his access as well as perform certain functions within the network. LAMO had access to individuals names and Social Security Numbers. LAMO informed The New York Times of the security vulnerability through SECURITYFOCUS.COM.

      LAMO has committed computer intrusions into several other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

      Each time LAMO commits a computer intrusion on a high profile organization he reports the vunerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

      LAMO has ties to former hacker [   ], who was arrested by the FBI for [   ]

b6   5
b7C   5
b5   2
b7E   5

Case ID : [   ]   [   ]

The New York Office and the Southern District of New York are currently investigating LAMO and his computer intrusions.

Descriptive Data:

        Main Subject
        Name -
          Last: LAMO
          First: ADRIAN
          Middle:
          Race: W
        Sex: M
        SOC: 042-74-6804
        Address -
          House #:   1230
          Street Name: Market Street, #106
          City: San Francisco
          State: CA
          Postal Code: 94102

 LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

It is requested to query logical sources and report only
positive intelligence regarding known or potential actions of   b6 -1
ADRIAN LAMO. Positive intelligence should be directed to SA   b7C -1

b6 -1
b7C -1

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 12/16/2002

To: New York   **Attn.:** C-37 Rotor
    New York   **Attn.:** SSA

From: New York
       Squad C-37
       Contact: A/SSA

Approved By:

Drafted By: 11m

Case ID #:

b3 -2
b6 -1
b7 -1
b7E -3

OPEN
SOURCE
DATE
SUPV
PI EFFECTIVE

SERIALIZED ___ FILED ___

DEC 1 8 2002

FBI — NEW YORK

UPLOADED
WITH TEXT
WITH/OUT TEXT
BY _____
DATE 12-30-02

FBI(19-cv-1495)-1739

b 3 2
I /E 3

Title: ADMINISTRATIVE AND MISSION MATTERS, SQUAD C-37
SQUAD PERSONNEL MATTERS

Synopsis: Request closing, reassignment, or completion/wrap up of the above listed cases.

Details: Due to EC dated 11/21/2002, the following personnel were transferred from C-37 to DT-5: SA [   ] SA [   ] [   ] SA [   ] SA [   ], SA [   ] SA [   ] SA [   ]

Based on a review of the below listed files, it was determined that investigation did not produce sufficient evidence of a crime. It is therefore requested that the following cases be administratively closed:

b6 -1
b7C -1
b3 -2
b7E -3

FILE NUMBER	Date Opened	# Serials	CASE AGENT
	09/08/02		
	07/10/02		
	08/01/01		
	11/01/01		
	08/01/02		
	07/26/02		
	07/10/01		

2

Based on a review of the below listed files, it was determined that additional investigative work is still to be completed. Therefore, the following cases will be reassigned:

FILE NUMBER	CASE AGENT	NEW CASE AGENT

b6 -1
b7C -1
b3 -2
b7E -3

3

b3   2
b7E   3

As the majority of investigative work has been
completed, the following cases will continue to be worked/closed
down by the originally assigned agent:

FILE NUMBER	CASE AGENT	STATUS
		Fully adjudicated, only evidence disposal issues
		Fully adjudicated, only evidence disposal issues
		Fully adjudicated, only evidence disposal issues
		Trial Prep, 01/03 Trial date

bC -1
b7C -1
b3 -2
b7E -3

The following leads were assigned months prior to the
DT-5 reassignment and will therefore stay with the original
assigned agent to be completed:

CASE ID	AGENT	Assigned
		08/19/2002
		09/21/1998

♦♦

4

b6 1
b7C 1

Reassignments

December 30, 2002

FROM   TO   FILE #

b6 -1
b7C -1
b3 -2
b7E -3

trans.wpc

UPLOADED

WITH/TEXT _____ ✓_____

WITHOUT TEXT_____

BY _____

DATE 2-7-03

Case transfer 2-7-03 ©

Classification changed 2-7-03 ©

SERIALIZED ___

2003

FOI -

b3 -2
b6 -1
b7C -1
b7E -3

(Rev. 08-28-2000)

L6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 02/05/2003

To: New York   Attn: C-37 Rotor
                                         DT-5 Rotor

From: New York
       Squad DT-5
       Contact: SA [   ]

Approved By: [   ] _m/m§M_

Drafted By: [   ] slf

Case ID #: [   ]

b)   2
b6   1
b7C   1
b7E   5

Title: ADRIAN LAMO;
        New York Times-Victim;
        Computer Intrusion;
        OO:NY

Synopsis: Change classification of above mentioned case and
transfer to DT-5

Details: Writer requests the above mentioned case classification
be changed to [   ] The investigation has revealed an
attack on the infrastructure of the United States' computer
networks with no financial basis.

b3   2
L7E   5

Since writer has been transferred to DT-5, writer requests the
above mentioned case be transferred to Squad DT-5 with the writer
as the case agent.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-13-2010 BY [ ] UC BAW LK RLS

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 12/10/2002

To: New York   **Attn:** SA [   ]

From: Miami
      C-6
      Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ]ajs

Case ID #: [   ]

b7   2
b6   1
b7C   1
b7E   3

Title: ADRIAN LAMO;
      NEW YORK TIMES-VICTIM;
      COMPUTER INTRUSION;
      OO:NY

Synopsis: Report findings to Case Agent.

Reference(s): [   ]

Enclosure(s): Copy of article titled "Inside the Hacker Mind" from NEW ARCHITECT magazine, December 2002.

Details: While conducting research via the Internet, writer discovered an article pertaining to ADRIAN LAMO. Per reference EC, enclosure is being forwarded to titled case agent for informational purposes and further investigation if appropriate.

b7   2
b6   2
b7C   1
b7E   3

SEARCHED _____ INDEXED _____
SERIALIZED _____ FILED _____

[ ] 2 2002

[ ] NEW YORK

b3   2
b7E   5

LEAD(s):

Set Lead 1:   (Adm)

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

2

FBI(19-cv-1495)-1747

[_____] wpd

UPLOADED
WITH/TEXT ✓
WITH/OUT TEXT _____
BY _____
DATE MAR 2 7 2003

JAN 1 3 2003

b¢ 1,5
b/C 1,5
b3 2
b/E 3

FD-302 (Rev 10-6-95)

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   01/14/2003

[   ] KINKO's, [   ]
[   ] telephone number [   ] was telephonically
contacted by the interviewing agent. After being advised as to the
identity of the interviewing agent and the purpose of the   b6 ⌐
interview, [   ] provided the following information: b7C ⌐

[   ] is not familiar with ADRIAN LAMO. [   ] stated
that he has recently [   ] a loss prevention intranet web-site
for KINKO's. [   ] further stated that once received he would
put a flyer about LAMO on their intranet site asking individuals
who have information about him to contact the interviewing agent.

b3 -2
Investigation on   01/14/2002   at New York, NY   (telephonically) b6 -1
                                                                                          b7C -1
File [   ]   Date dictated 01/14/2002   b7E -3

by SA [   ]

FBI(19 cv 1495) 1/49

UPLOADED
WITH/TEXT _____
WITH/OUT TEXT _____
BY _____
DATE _____ MAR 2 7 2003

SERIALIZED [ ] . FILED _____

JAN 2003

b6   1,5
b7C   1,5
b7D   2
b7E   3

FD-302 (Rev 10-6-95)

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   01/14/2003
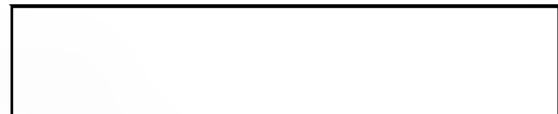
[ ] KINKO's, [ ] San
Francisco, CA, telephone number [ ] was telephonically
contacted by the interviewing agent. After being advised as to the
identity of the interviewing agent and the purpose of the
interview, [ ] provided the following information:

b6 -
b7C -

[ ] is familiar with the name ADRIAN LAMO. [ ] has
seen flyers with LAMO photograph on them in several of the San
Francisco, CA area stores. [ ] stated to please send him
information pertaining to LAMO and he will query his other stores
to see if they have any knowledge of LAMO.

Investigation on 01/14/2002 at New York, NY   (telephonically)

b6 2
b6 1
b7C
b7E

File # [ ]   Date dictated 01/14/2002

by SA [ ]

FBI(19-cv-1495)-1751

JAN

b6   1
b7C   1
b5   2
b7E   3

Out

b3 -1
b6 -1
b7C -1

To: [   ]
Subject: Subpoena request: Attn: [   ]

Hi, [   ]:

I am not sure if you remember speaking to me regarding the Adrian Lamo investigation several months ago. We are still continuing to investigate his activities. One of the things I have done since we last spoke was send some of our Agents to interview employees [   ] [   ] regarding Lamo. They were mostly attempting to determine if Lamo utilized their facilities. In speaking to several of the managers of the stores, the Agents were informed that [   ] and referred us to your legal department. We [   ] [   ] In the interium, I have spoken to [   ] who has ultimately referred me to you regarding this issue. She informed me that you have a copy of the subpoena and would be able to provide me with the information. What the subpoena requests is:

b3   1
b7E   1
b6   1,6
b7C   1,6

I was wondering if you had this information available and if you could email it to me. If you have any questions please call me at [   ]

Thank you for your time and help,

[   ]

KinKos.wpd

UPLOADED
WITH/TEXT ✓
WITH/OUT TEXT
BY
DATE   APR   2 2003

JAN 14 2003
FBI

b6 -1,5
b7C -1,5
b3 -2
b7E -3

FD-302 (Rev 10-6-95)

-1-

b6   1
b7   1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   01/14/2003

[ ] Paralegal, KINKO's LEGAL UNIT, telephone number [ ] was telephonically contacted by the interviewing agent. After being advised as to the identity of the agent and the purpose of the interview, [ ] provided the following information:

b6 -5
b7C -5

[ ] stated that there are loss prevention managers that [ ] KINKO'S. [ ] telephone number [ ] Eastern Coast including Washington, DC, [ ] telephone number [ ] Pennsylvania and [ ] telephone number [ ] San Francisco, CA.

Investigation on   01/14/2002   at New York, NY

File # [ ]

Date dictated   01/14/2002

by   SA [ ]

b3 -2
b6 -1
b7C -1
b7E -3

FBI(19 cv 1495) 1/55

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Soft.wpd

Soft.wpd

UPLOADED
WITH/TEXT _____
WITHOUT TEXT _____
BY _____ APR 4 2003
DATE _____

SERIALIZED _____ FILED _____

FEB 2003
FBI - _____

bc -1
b7C -1
b3 -2
b7E -3

(Rev. 08-28-2000)

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 02/21/2003

To: New York   Attn: FMU
                                      MIS

From: New York
      Squad DT-5
      Contact: SA [   ]

Approved By: SAC BILLY, JOSEPH JR
             ASAC [   ]
             CSSA [   ]
             SSA [   ] PJD/LKW

b6   2
b6   1
b7C
b7E   5

Drafted By: [   ] slf

Case ID #: [   ]

Title: ADRIAN LAMO;
       New York Times-Victim;
       Computer Intrusion;
       OO:NY

Synopsis: Request for case fund expenditure

Enclosure(s): One (1) copy of comparision price listing for
requested software

Details: ADRIAN LAMO is the subject of the above mentioned
computer intrusion investigation.

In February 2002, LAMO discovered several misconfigured proxy
servers acting as doorways between the public Internet and the
New York Times' private intranet. LAMO utilized the proxy
servers to gain access to the New York Times network. Once on
the network, LAMO cracked a password for a userid with supervisor
rights. Utilizing this userid he was able to broaden his access
as well as perform certain functions within the network. LAMO
had access to individuals names and Social Security Numbers.
LAMO informed The New York Times of the security vulnerability
through SECURITYFOCUS.COM.

        LAMO has committed computer intrusions into several
other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME
and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for
proxy servers that are misconfigured. Once he obtains this
information, he configures his browser to appear and utilize the
proxy server as his own. Once the computer intrusion occurs,
LAMO searches the network to determine if there are any other

vulnerabilities and in the case of The New York Times, left a
backdoor so that he could enter at another time undetected.

Each time LAMO commits a computer intrusion on a high
profile organization he reports the vunerability and intrusion to
the media causing a distrust of the company's clients. The above
mentioned corporations have lost significant money and trust of
their clients.

Due to the specific technical needs of the [   ]
investigation, it is necessary for the software [   ] to
be purchased. The software is a necessary component needed to
continue and complete the investigation.

b7E 1, e

The current budget balance in captioned case is
[   ] allowing these payments, the case budget will be
[   ]

♦♦

loss.wpd

APR 0 1 2003

b6 -1
b7C -1
b3 -2
b7E -3

01/14/2003
CAH:cah

b6   1,5
b7C   1,5
b5   2
b7E   3

The attached emails were sent to [   ] telephone number [   ]
email: [   ] and [   ] telephone number [   ] email:
[   ] pertaining to ADRIAN LAMO.

To: [redacted]
From: SA [redacted]
Subject: Adrian Lamo
Cc:
Bcc:
Attached:

b6 -1, 5
b7C -1, 5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-10-2010 BY [redacted] UC BAW/DK RYC

Hi, [redacted]

   As per our conversation, I have attached a flyer of Lamo with detailed information about him and the investigation. As I stated in our telephone call, it is known that Lamo utilizes Kinko's services to access the internet in order to commit unauthorized intrusions of corporations. Once Lamo does these intrusions, he does contact the companies through a third party but it is not until he reports the vunerability to the media first given other hackers the opportunity to get in the compromised system. Also, Lamo is usually in the system for a long period of time before he contacts the company to let them know of the vunerability.

   Lamo does not have a steady home address. He frequents the states of California, Texas, New York, Pennsylvania and Washington, DC/Virginia. When he performs his hacks he usually utilizes his own laptop computer, so some of the Kinko's he is using have internet access for laptops.

   I appreciate all of your help on this investigation. If there is anything you ever need from my end please let me know. I can be contacted at [redacted], cell: [redacted] and email [redacted]

b6 -1
b7C -1

Sincerely, [redacted]
SA [redacted]

b6   1
b7C 1

To: [ ]
Subject: Adrian Lamo

bo -1,5
b7C -1,5

Hi, [ ]

Thank you for taking the time to speak with me today, I really appreciate it. After I spoke with you I contacted [ ] who was also very helpful. He told me to forward him the attached flyer, which I did and he will get the okay to put it on your loss prevention intranet web-site. He also stated that he will query the areas where Lamo frequents for further information.

I just wanted to let you know so that you both and not doing duplicate work. I have attached the flyer for your information. My contact information is [ ] FBI New York, [ ] cell: [ ]

Thanks again for your help. If you ever have any questions please feel free to call me.

Sincerely,
Special Agent [ ]

be 1
b7C 1

trans1.wpd

UPLOADED

WITH/TEXT

WITH/OUT TEXT

BY

DATE APR 1 4 2003

bo -1
b7C -1
b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 3-17-   BY   U BAW (BL?

b6   1
b7C   1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 04/06/2003

To: New York

From: New York
Squad DT-5
Contact: SA [   ]

Approved By: [   ]

Drafted By: [   ]slf

Case ID #: [   ]

b3 -2
b6 -1
b7` -1
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

Synopsis: Change classification of above mentioned case and
transfer to DT-5

Details: Writer requests the above mentioned case classification
be changed to [   ] The investigation has revealed an
attack on the infrastructure of the United States' computer
networks. The subject is within the United States and is not
state sponsored.

b3 -
b7E -

♦♦

insert2.wpd

bo -1
b7 -1
b3 -2
b7E -3

05/07/2003
CAH cah

The attached email was received from [   ] from [   ] regarding the subpoena served on them requesting any/all documentation pertaining to the computer intrusion by ADRIAN LAMO.

A copy of the email and file will be maintained in the file.

b3   1,2
b6   1,5
b7C 1,5
b7E 3

Subject: FW: Grand Jury Subpoena: Adrian Lamo
To: [ ]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-__-2010 BY [ ] UC BAW/DK RY3

-----Original Message-----
From: [ ]
Sent: Tuesday, May 21, 2002 1:39 PM
To: [ ]
Subject: Grand Jury Subpoena: Adrian Lamo

bo -1, 5
b7C -1, 5
b7D -1

Agent [ ]

    In response to the grand jury subpoena your Office served on the Company, attached are files that were given to [ ] by Mr. Lamo as [ ] These records are being produced with the understanding that the information will be used solely for your criminal investigation and for no other purpose.
I am sending the two files separately because of storage limitations on your e-mail account.

bc 5
b7C 5
b7E 1
b   1
b7D 1
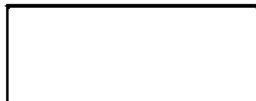
bo -1
b7 -1

Printed for SA [ ]

5/7/2003

one302.wpd

b6   1
b7C   1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   06/09/2002

[_____] and [_____] legal
counsel, WORLDCOM, were telephonically contacted, [_____] by
the interviewing agent. After being advised as to the identity of the
interviewing agent and the purpose of the interview, the following
information was obtained:

b6 -2, 5
b7C -2, 5

[_____] stated that WORLDCOM's first awareness that ADRIAN L. b7D -1
had gained unauthorized access into their network was a voicemail left
for [_____] Public Relations office. [_____] spoke with [_____]
[_____] Securityfocus.com. [_____] told [_____] that LAMO had
contacted him and informed him that he had hacked into WORLDCOM.
[_____] informed [____] that he could put her in touch with LAMO if
necessary. [_____] contacted [_____] [_____] is the
[_____] Information Systems.

[_____] and [_____] work for [_____] They along with [_____]
telephonically contacted LAMO at (415) 505-4225. [_____] stated that
LAMO told him he was willing to meet with them and requested them not
to prosecute him for hacking into their network. A non-disclosure
agreement was completed by WORLDCOM and LAMO regarding this incident.
LAMO later revealed information to the press breaking a stipulation
in the non-disclosure.

On 12/1/2001, they had their first telephone call with LAMO.
LAMO informed them he had found the open proxy server in October 2001
but he had other things to do and did not get back to exploiting the
opening until a few weeks later.

Through several telephone calls, two (2) on Saturday, December
1, 2001 and one (1) on Tuesday, December 4, 2001, LAMO provided them
with the hacking methods he had used to gain unauthorized access into
their network, the Internet Protocol (IP) addresses he hit and screen
captures of WORLDCOM's internal network. LAMO specifically stated
that he utilized an open proxy on WORLDCOM's network to gain his
unauthorized access to their network. [_____]
[_____] It is through
this information provided that the team was positive it was LAMO who
had hacked into their network.

b7E -1
b7D -1

Investigation on	06/07/2002	at New York, NY	(telephonically)

b3 -2
b7E -3

Continuation of FD-302 of ___Conference Call___, On _06/07/2002_, Page __2__

Once in their network, LAMO had the power to access WORLDCOM's system[   ]   LAMO had obtained enough information [   ] [   ] LAMO left footprint in files on the machines he compromised.

[   ] stated that LAMO was never an employee of WORLDCOM nor was he ever provided authorized access into their network. They were familiar with [   ] because he had hacked them in the past and was arrested for his crime.

WORLDCOM sustained damages totaling approximately $500,000 resulting from the unauthorized intrusion by LAMO.

b7E -1
b6 -2, 5
b7C -2, 5
b7D -1

dist2.wpd.

MAY 07 2003

b6 -1
b7C -1
b3 -2
b7E -3

05/07/2003
CAH.cah

bo   1,2
b7C   1,
b3   2
b7E

    SA[   ]received the attached email from[   ]
WORLDCOM/MCI. There was an attached file containing information pertaining to the
unauthorized intrusion of ADRIAN LAMO into WORLDCOM.

    A copy will be maintained in the file.

Subject: RE: Adrian Lamo
To: 'SA[   ]

[   ]

Attached is the second file of screenshots that Adrian provided as proof he
was in the[   ] :-)

~~~~~~
[   ]
[   ] Network Security Ops Ctr
[   ]
[   ]
~~~~~~

-----Original Message-----
From: SA[   ]
Sent: Wednesday, May 07, 2003 12:56 PM
To:[   ]
Subject: Adrian Lamo

It has been a year since I last spoke with you regarding Adrian Lamo. So
much has happened in that year on my end as I am sure on your end. So how
are you doing? We have been so busy here that I had to put this case on
the back burner for awhile but now we are getting ready to go forward with
the case and present it to a Grand Jury. I am in the process of getting
everything organized so that we can do that. With that said I just wanted
to make sure of a couple of things:

1. About a year ago you sent me an email with[   ] You told
me you were going to send a second file.[   ]
[   ] At the time, I did not have an fbi.gov account and the
email account I was using was restricted in size. I have been reviewing
all of the material and I do not see the second email with the file
attached. I was wondering if you still have this file and if so could you
forward it to me. I believe it is[   ]

2. The second question I have is are[   ] and[   ]
[   ] still working for WorldCom?

I can imagine how busy you are and I appreciate any help with this
matter. As I informed you from the beginning I will keep you informed of
all steps forward in this case. I have a meeting with the United States
Attorney today to discuss the Grand Jury proceedings. I will email you
with an update. I believe at this junction things will be moving forward
very quickly to bring this investigation to a resolution.

If you need to contact me by telephone my number is[   ]

Thanks,

b6 -1,2
b7C -1,2
b7E -1

b3 1
b6 2
b7C 2
b7E 1

b6 1
b7C 1

Printed for SA

NYtimesert.wpd

UPLOADED
WITH/TEXT ✓
WITH/OUT TEXT
BY DL
DATE MAY 9 2003

NYtinsn1.wpd

MAY 0 7 2003

b6 -1
b7C -1
b3 -2
b7E -3

b6 -1
b7C -1
b3 -2
b7E -3

05/07/2003

SA[ ]received the attached emails from[ ]
[ ]and[ ]of THE NEW YORK TIMES.

[ ]followed up with a question sent to him via email by SA[ ]asking if
any[ ]were sent up by ADRIAN LAMO when LAMO gained unauthorized access
to their system. The answer to this question was that no accounts were generated at this time.

b6 -1,2
b7C -1,2
b7E -1

[ ]followed up with several questions stating that the home address and social
security numbers for all the staff were accessible to LAMO and that is how he was able to gain
superuser access.

[ ]provided a NEW YORK TIMES article referencing LAMO.

Copies will be maintained in the file.

Subject: Lamo
To:

Sorry I forgot to send this NY Times article to you.

b6 -1,2
b7 -1,2

April 28, 2003

A New Way to Catch a Hacker

By NICHOLAS THOMPSON

   or a computer security professional, Lance Spitzner has an unusual
goal: He wants ill-intentioned hackers to steal more Social Security
numbers and medical
   records.

Mr. Spitzner, a former Army officer, spends his days working at Sun
Microsystems and his evenings running the volunteer Honeynet Project, a
group of security
professionals working to track hackers. Until recently, the four-year-old
nonprofit effort focused on building and monitoring honeypots ? computer
systems designed
to be easily penetrated so that Honeynet volunteers can covertly scrutinize
hackers' tricks when they break into the systems.

Now Mr. Spitzner, 32, is focusing his efforts on a different type of
defense based on the insertion of "honeytokens" into real databases and
systems.

Honeytokens are pieces of seemingly enticing information that have no
useful value. Embedded in ways so that no innocent person should
accidentally stumble upon
them, honeytokens trigger alarms when viewed, grabbed or downloaded. For
example, a bank could insert a fake credit card number into its files and
then set up a
program called a "sniffer" on the network that would send out an alarm if
anyone touched that particular number.

The term "honeytokens" was coined on Feb. 21 by a programmer named Augusto
Paes de Barros who used it in an e-mail message to a list of security
professionals.
But the idea is not new.

It dates back in computing at least to 1986, when Clifford Stoll, a
programmer at Lawrence Berkeley National Laboratory in California, buried
fake records for an
organization called the Strategic Defense Initiative Network deep in his

b6 -1
b7C -1

server. When intruders started downloading the records, and then someone sent a letter to Mr.
Stoll about the phony organization, he and federal investigators traced the intruders to East German and Soviet intelligence agencies.

Today, the use of honeytokens is not uncommon. For example, ForeScout Technologies, based in San Mateo, Calif., has built a commercial software program that
tracks incidents of surreptitious reconnaissance, like port scans ? the computer equivalent of someone turning your doorknob to see if it is unlocked. The program
will announce a false message of vulnerability to the scanner in the form of a honeytoken. It then breaks the connection if the hacker follows up with an attack.

Honeytokens, like their cousins the honeypots, are based on the notion that if you build it, they will come. Mr. Spitzner became intrigued by the idea of honeypots
after putting a new computer online at home and watching it get attacked within 15 minutes by an automatic program scanning the Internet for vulnerable prey.

Many computer criminals break into systems simply for the fun and challenge. Others are looking to take over vulnerable systems in order to use them as safe houses
for setting off further, more serious, attacks. Others want to mine credit card addresses or steal corporate secrets. According to a 2002 report by the Computer
Security Institute, 90 percent of the 500 corporations, government agencies, financial institutions, medical institutions and universities surveyed detected security
breaches during the previous year.

Honeytokens could also be useful for national security purposes. Michael Vatis, director of the Institute for Security Technology Studies at Dartmouth University, said
that the Defense Department could use them to snare people seeking unauthorized information on weapons systems. For example, a honeytoken could be designed so
that if it were downloaded and then taken to a different system, it would be able to contact its original server each time it was accessed. One way to do this would be
to include code in the honeytoken that would automatically try to fetch a tiny image or some other file based on the home server, making the honeytoken "phone
home" whenever it is opened.

Honeytokens also can be used to track attacks from within a company by people who have passwords to enter the system legitimately. Pete Herzog, managing
director of the Institute for Security and Open Methodologies, says that he

b(1
l /C   1

has used honeytokens to detect when employees illicitly download forbidden material. For
example, he has entered corporate memos with particular typos into private
databases and then monitored company networks to see where those typos show up.
Tracing these honeytokens, he says, often leads to caches of illegal
materials stored on the network.

No one believes that honeytokens can stop all cybercrime. But they could
offer an upgrade in protection.

Honeytokens offer another advantage: They help reduce the number of false
positives in other cyberdefense systems. Like car alarms, intrusion
detection systems can
go off so frequently because of accidental trespassing that many security
administrators ignore the warnings. Honeytokens, if designed correctly,
should trigger alarms
only if there is a malicious attack.

Hackers, however, are not impressed. Adrian Lamo, who gained notoriety last
year when he claimed to have broken into the systems of a number of
companies,
including Yahoo, says he is not worried. "It's a form of old-school
security," he says. "It will work on the people who have been to the old
schools."

Mr. Lamo says that he only goes after information that he knows other
people frequently seek access to and that he runs credit checks to ensure
that information he
uncovers, like Social Security numbers, are real. Mr. Spitzner contends
that it should not matter whether a hacker bothers to run a credit check
because the alarm
should ring any time the decoy record is accessed.

Hackers can also evade honeytokens by compressing and password-protecting
the information they steal, thereby changing or hiding the data, like fake
Social
Security numbers or typos, in memos that the sniffers are searching for.
And "phone home" honeytokens designed to trace users could be thwarted if
opened only on
computers disconnected from the Internet.

Some experts are also worried about the possibility that using honeytokens
could violate the federal Wiretap Act, which places limits on intercepting
and monitoring
electronic communications. Richard Salgado, senior counsel for the Justice
Department's computer crime and intellectual property unit, has said that
very little law
governs this new area and that security technicians should consult first
their lawyers.

bC -1
b7C -1

Printed for SA

Mr. Spitzner said that he was less worried about the law than about smart hackers. Honeytokens cannot solve all problems, he said. "But they can make a very simple and powerful tool in a security arsenal."

b6 -1
b7C -1

To: [redacted]
Subject: RE: Adrian Lamo

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-15-_- BY [redacted] [redacted]

Ms. [redacted]

b6   1,2
b7C   1,2

There are numerous areas to access and he appeard to have tried all or most of them.

The staff list showed home addresses and social security numbers for all staff.
There were metro and op-ed source lists. In some cases op-ed entered social security numbers in the source lists.

Regards,

[redacted]

b7E -1
b6 -1,2
b7C -1,2

-----Original Message-----
From: [redacted] /NYT/NYTIMES [mailto: [redacted]
Sent: Tuesday, May 06, 2003 2:41 PM
To: [redacted] /SYS/NYTIMES; [redacted] /CORPHQ/NYTIMES; [redacted]
[redacted]
Cc: [redacted] CORPHQ/NYTIMES; [redacted]
Subject: Re: Adrian Lamo

Folks:

As requested, can you please respond to Special Agent [redacted] questions. Her e-mail address is [redacted]

Thank you.

[redacted]
----- Forwarded by [redacted] NYT/NYTIMES on 05/06/2003 02:36 PM -----

SA [redacted]
To: " [redacted]
[redacted] NYT/NYTIMES" [redacted]
[redacted]   cc:
>   Subject: Re: Adrian Lamo

b6 -1,2
b7C -1,2

05/06/2003 01:27
PM

Printed for SA [redacted]

Hi, [ ]

I know we have been playing phone tag.= I have a meeting in about 10 minutes so I will try to call you after I get out of the meeting.= I have been going through all the information and evidence from the New York Times and Lexis/Nexus and I have the following questions for the mentioned individuals.= I think these will be the final questions for now.= If you could just forward them onto the appropriate individuals for comment, I would greatly appreciate it.

b6 4,5
b7C 4,5
b7E 1

b6 1
b7C 1

b / E   1

16   1,2
b /C   1,<
L /E   1
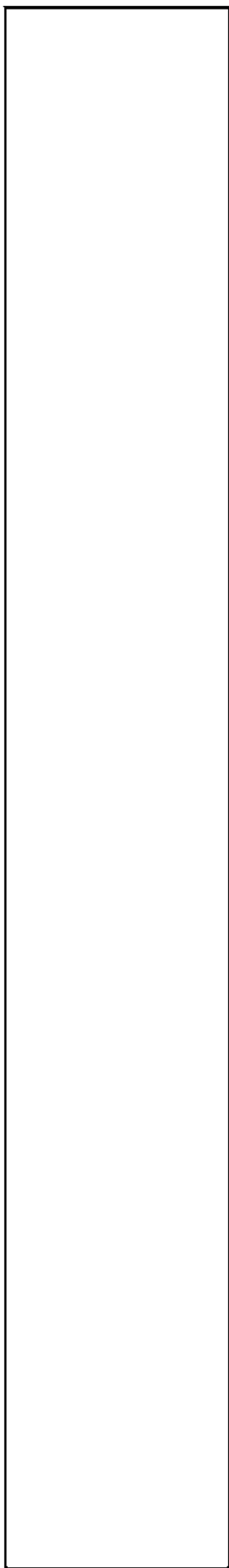
═══ Thanks ☐ ═ I will call you in alittle while.═ I appreciate all your help.

☐

16   1
b /C   1

FD-302 (Rev. 10-6-95)

- 1 -

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   08/29/2002

[   ] SBC, email: [   ] telephone number: [   ], was telephonically contacted by the interviewing agent. After being advised as to the identity of the interviewing agent and the purpose of the interview [   ] provided the following information:

b6 -2
b7C -2

[   ] is familiar with unauthorized intrusion of SBC by hacker ADRIAN LAMO. [   ] stated that another SBC employee, [   ] telephone number [   ], was approached by a Newsbytes reporter. The Newsbytes reporter stated that a white hat hacker had contacted him and informed him that he had gained unauthorized access to SBC's network. Through emails, the reporter identified the hacker as LAMO. The reporter further stated that LAMO was able to see all their customers' information. LAMO utilized a vulnerability in the dial up pools of SBC's customers. He gained access to their network by opening up his Netscape browser and typing in a particular Internet Protocol (IP) address and keyword. This action caused an URL attack to occur causing SBC's index of files to be displayed in LAMO's browser. The index feature must be turned on for this to occur. LAMO claimed the vulnerability to their system was in their dial up routers.

LAMO was able to view customer account names, passwords and email addresses. Over 3600 customer's were vulnerable to the attack.

The technical team at SBC was able to validate the vulnerability LAMO had utilized. They went through their directory structure to determine the amount of damage LAMO had inflicted. The technical team had to call all 3600 customers individually and change all of their passwords. The web server and dial up logs were preserved. Some of the IP addresses in the web server logs resolved to Kinko's stores. Other IP addresses resolved to dial up accounts.

[   ] and [   ] had indirect contact with LAMO. They decided not to speak to him directly. [   ] is unaware if anyone from SBC's Public Relations Department spoke to him directly. About two (2) to three (3) weeks later, an individual who works in their security department was approached by LAMO via email. The

b3 -2
b6 -1,2
b7C -1,2
b7E -3

Investigation on   08/27/02   at   New York, NY   (telephonically)

File # [   ]   Date dictated   08/29/02

by SA [   ]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency

b6
b/C
b>
b/E

email stated that LAMO was not satisfied with the way SBC handled
his unauthorized intrusion announcement and he wanted to speak with
someone at SBC. They did not contact him at this time.

In July 2002, LAMO contacted an individual at SBC. LAMO
stated that he had further information to provide to SBC. They
asked him to write to them regarding this new information. LAMO
never contacted them again.

lettergav.wpd

bo -1
b7C -1
b3 -2
b7E -3

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No

26 Federal Plaza
New York, NY 10278

May 13, 2003

Senate Legal Counsel
642 Senate Hart Building
Washington, DC 20510
RE: ADRIAN LAMO, Hack of website www.senate.gov

b6   6
b7C 6

Dear

As per our conversation on 12/28/2003, I am writing to
request information pertaining the unauthorized intrusion of the
website www.senate.gov in December 2003. Investigation by the
FBI's New York office has revealed that the individual ADRIAN
LAMO is responsible for this unauthorized intrusion.

LAMO is a subject of an ongoing investigation by the
FBI's New York office. LAMO has claimed credit for the
unauthorized intrusions into The New York Times, Worldcom,
Microsoft, Yahoo, AOL, SBC Communications and excite@home.com
through open proxy servers. LAMO uses a "Proxy Hunter" to search
the Internet for proxy servers that are misconfigured. Once he
obtains this information, he configures his browser to appear and
utilize the proxy server as his own. Once the computer intrusion
occurs, LAMO searches the network to determine if there are any
other vulnerabilities. LAMO has left backdoors in the networks
providing him with the ability to enter the network at another
time undetected.

The enclosed article dated 12/10/2002 from
Securityfocus.com states that LAMO gained access to
www.senate.gov through an open proxy server. TRACY WILLIAMS,
Director of technology development for the Sergeant-at-Arms,
blamed the incident on misconfigured devices associated with the
Web site and that the devices were taken off line until they
could be configured correctly.

The FBI's New York Office is requesting all records and
other evidence in the possession of www.senate.gov. Such records
and evidence include, but are not limited to, all accounts,
computer logs, files, communications, E-mail messages, programs,
client account records and files, and any other documents: worked
on, reviewed by, drafted by, edited by, examined by, received by,

sent to or pertaining to the unauthorized intrusion by in December 2002. The FBI's New York Office is also requesting to speak with the individuals who handled the investigation into the unauthorized intrusion into the proxy server and web-site as well as the individual who had contact with LAMO.

Your efforts in this matter will help to ensure that the privacy and integrity of the information contained within www.senate.gov will be maintained.

Please contact SA [   ] regarding this matter at [   ] or email: [   ] Please note, the aforementioned information is sensitive in nature, not meant of external distribution.

bt   1
b/C   1

Sincerely,

Kevin P. Donovan
Assistant Director in Charge

By: [   ]
Supervisory Special Agent

2

SecurityFocus™

My Account | About Us | Media Kit

Entire Site

SecurityFocus

Wonder what SecurityFocus had to say last w

Sign up for weekly SecurityFocus newsletters t

| Home | The Basics | Microsoft | UNIX | IDS | Incidents | Virus | | Sign In |

Bugtraq · Forums & Newsletters · Library   Free Analyzer Download

<< Printable version >>

NEWS

Senate Closes Accidental Anonymizer

By *Kevin Poulsen*, SecurityFocus Dec 10 2002 1:24PM

Never let it be said that the United States Senate has done nothing for Internet privacy.

Network administrators for the U.S. government site www.senate.gov shut down an open proxy server over the weekend that for months had turned the site into a free Web anonymizer that could have allowed savvy surfers to launder their Internet connections so that efforts to trace them would lead to Capitol Hill.

A proxy server is normally a dedicated machine that sits between a private network and the outside world, passing internal users' Web requests out to the Internet. But they're sometimes misconfigured to accept and forward connections from the outside as well, allowing anyone on the Internet to route through the proxy with a simple browser configuration change.

Because server logs at destination sites show only the IP address of the proxy server, and not the end user, some hackers and privacy-conscious netizens catalog open proxies and use them to anonymize their surfing.

Tracy Williams, director of technology development for the Senate Sergeant-at-Arms, blamed the Senate's accidental public service on misconfigured devices "associated" with the Web site. "Those have been taken offline until they can be configured correctly," said Williams.

Although open proxies sometime allow unauthorized ingress to an internal network, Williams said that in this case the Senate's networks were not exposed.

The proxy was discovered by hacker Adrian Lamo, who's still free, and wandering the San Francisco Bay Area with a new laptop.

The hacker said he noticed the Senate Web site's undocumented feature while reviewing a list of proxy servers he scanned and cataloged last April. Uncharacteristically, Lamo said he made no effort to hack the Senate's internal network through the system. Instead, late last week he used it to send a message to any administrators monitoring the site.

senate.gov wpd

SERIALIZED FILED

MAY 1 2003

b3 -2
b6 -1,6
b7C -1,6
b7E -3

FD-302 (Rev. 10-6-95)

bo -1
b7C -1

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   12/30/2002

[   ], Senate Legal Counsel, 642 Senate Hart
Building, Washington, DC 20510, telephone number [   ]
was telephonically contacted by the interviewing agent. After   bt
being advised as to the identity of the interviewing agent and the b7C o
purpose of the interview, [   ] provided the following information:

[   ] stated that the website www.senate.gov was recently
hacked. [   ] stated that she has spoken to the technical
individuals involved in investigating the unauthorized intrusion
into the website. [   ] has requested the FBI to send a request in
writing to her enabling the interviewing agent to speak with the
individuals involved in the investigation.

b3 -2
b6 -1

Investigation on   12/28/02   at New York, NY   (telephonically) b7C -1

File # [   ]   Date dictated 12/30/02   b7E -3

by   SA [   ]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency;
it and its contents are not to be distributed outside your agency.

FBI(19 cv 1495) 1/95

Calls.wpd

UPLOADED

WITH/TEXT ✓

WITH/OUT TEXT

BY

DATE MAY 1 4 2003

MAY 2003

b3
b6 1
b7C 1
b7E 3

b3   2
b6   1
b /C   1
b /E
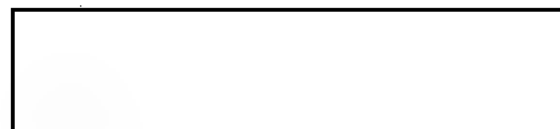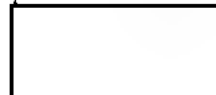
05/13/2003
CAH:cah

SA[_____] has made the following telephone contacts and emails on the dates specified for the above mentioned case number:

05/13/2003   Called and left message for[_____]NBC[_____], regarding technical contact for Lamo hack

b6   1,2
b /C   1,2

05/13/2003   [_____]The New York Times, contacted informed of upcoming complaint and asked for[_____]to contact[_____]at[_____]

05/13/2003   [_____]SBC,[_____]called after I left him a message. Stated he would send me the logs I requested regarding Adrian Lamo. He left his email address of [_____] SA[_____]sent[_____]an email   A copy is attached.

To: [ ]
From: SA [ ]
Subject: Questions about Lamo
Cc:
Bcc:
Attached:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-10-2010 BY [ ] UC BAW/CK R1S

b6   1,2
b7C   1,2

Hi, [ ]

   Here are a couple of questions I came up with when reviewing the information you provided to me last August. I am sorry if some of them are repetitive I am just trying to get things in order. I think this will be it unless I have some questions about the logs.

2. Can you find out if anyone in your PR Dept spoke with him directly about the Feb 2002 incident?

3. Do you have any of the emails that Lamo sent to you[ ] and/or the individual in the security unit?

b6 -1,2
b7C -1,2
b7E -1

6. Who from Newsbytes 1st contacted you, [ ] and on what date?

I think that is it. Thank you again for your help.

Best wishes,

[ ]

d

UPLOADED
WITH TEXT ___ ✓
WITHOUT TEXT _____
BY ___ [signature] MAY 1 4 2003
DATE _____

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-15-2___ BY [ ] TW BAW/KBS

MAY 1 3 2003

b3   1, -
b6   1
b7C   1
b7E   3

05/13/2003
CAH:cah

b6   1,5
b7C   1,5
b3   1,2
b7E   3

SA[   ] contacted [   ] telephone number [   ] [   ] email: [   ] regarding the subpoena request for information pertaining to ADRIAN LAMO. [   ] stated that the case is assigned to a case worker and that he would have the case worker contact me today regarding this matter.

far.wpd

UPLOADED

WITH/TEXT _____✓_____

WIT./OUT/TEXT _____

BY _____OL_____

DATE ____MAY 2 0 2003____

SERIALIZED _____OL_____ FILED _____

MAY 1 2 2003

b3 -2
b6 -1
b7C -1
b7E -3

05/20/2003
CAH:cah

b3 -2
bo -1
b7 -1
b7E -3

    The attached list and CD-Rom contains files that were extracted from a TAR file sent to us by Lexis-Nexus regarding the computer intrusion of ADRIAN LAMO

    A copy will be maintained in the file.

wpd

SERIALIZED _____ FILED _____

JUN 1 2 2003

b3 -1,2
b6 -1
b7C -1
b7E -3

- 1 -

FEDERAL BUREAU OF INVESTIGATION

b6 -1
b7C -1

Date of transcription   06/12/2003

[_____] General Counsel, T-Mobile, 4120
International Parkway, Suite 1000, Carrolton, TX 75007, telephone
[_____] facsimile (972) 930-4741, email: [_____]
[_____] was telephonically contacted by the interviewing agent. b6   6
After being advised of the identity of the interviewing agent and b7C   6
the purpose of the interview, [____] provided the following
information:

      T-Mobile provides the Wi-Fi Internet service for
Starbucks. In order to use a T-Mobile hotspot at a Starbucks you
must either be an existing T-Mobile hotspot customer or you can
provide Starbucks with a credit card number and be a "pay as you
go" customer. All customers receive a userid and password to sign
into the Wi-Fi service. [_____] stated to review the website www.t-
mobile.com/hotspot for more details regarding the service.

[_____] stated that [_____]
[_____] was
unable to provide [_____]
[_____] [____] stated he would need to refer me to a
technical person for this answer.

b6 -6
b7C -6
b7E -1
b3 -1

Investigation on	06/12/2003	at New York, NY	(telephonically)

b3   2
b6   1
b7C 1
b7E 3

File # [_____]

Date dictated 06/12/2003

by SA [_____]

FBI(19-cv-1495)-1804

insert2.wpd

UPLOADED
WITH/TEXT
WITH/OUT TEXT
BY
DATE   JUN 1 8 2003

JUN 1 2 2003

b3 -2
b6 -1
b7C -1
b7E -3

06/11/2003
CAH cah

be   1,[
b/C   1,2
b3   2
b/E   3
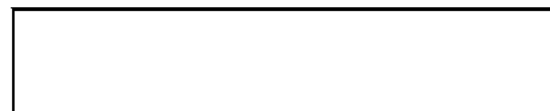
[____]LOCK/LINE, INC, telephone number [____] was telephonically contacted by SA[____]regarding the hack by ADRIAN LAMO of CINGULAR. LOCK/LINE, INC hosts the servers for CINGULAR that were hacked by LAMO. [____] referred SA[____]to their General Counsel,[____] telephone number[____]stated that he was the technical person involved in the hack by LAMO on their servers [____] stated he is familiar with LAMO's past hacking activities.

SA[____]attempted to contact [____]but met with negative results. [____]will be out of the office until 6/13/2003.

insert1.wpd

UPLOADED

WITH/TEXT ✓ _____

WITH/OUT TEXT _____

BY _____

DATE _____ JUN 1 8 2003

WIRED NEWS

Home | Technology | Culture | Business | Politics | Wired Mag | Animation   Text Size: A A A A

Lamo Hacks Cingular Claims Site

By Christopher Null | Also by this reporter

10:55 AM May. 29, 2003 PT

Cingular can issue insurance to its mobile-phone customers to protect them against loss and damage, but it apparently can't ensure that hackers won't have full access to their personal data.

Adrian Lamo, a hacker who in the past has broken into *The New York Times* and Yahoo, found a gaping security hole in a website run by a company that issues the insurance to Cingular customers. By accessing the site, Lamo said he could have pulled up millions of customer records had he wanted to.

He said he discovered the problem this weekend through a random finding in a Sacramento Dumpster, where a Cingular store had discarded records about a customer's insurance claim for a lost phone. By simply typing in a URL listed on the detritus, Lamo was taken to the customer's claim page on a site run by lock\line LLC, which provides the claim management services to Cingular.

Normally, this page should have been reachable only by passing through a password-protected gateway, but by simply entering the valid URL, Lamo discovered that individual claims pages could be accessed, no password authentication needed.

Each page contained the customer's name, address and phone number, along with details on the insurance claim being made. Altering the claim ID numbers (which were assigned sequentially) in the URL gave Lamo access to the entire history of Cingular claims processed through lock\line, comprising some 2.5 million customer claims dating back to 1998.

Lamo said the hack was similar to his discovery of a security hole at Microsoft in October 2001, where the server was configured to assume that if a user could reach a certain URL that was otherwise unpublished on the Internet, that user must be authorized to do so and must already be logged in.

As with his other hacks, Lamo said he had no intent of profiting from the exploit, just pointing out a security flaw.

Lamo first exposed the problem to Wired News. After this reporter pointed out the flaw, Cingular and lock\line closed the hole by Wednesday morning.

Cingular spokesman Tony Carter said lock\line has enabled password protection for the site and has now incorporated "obfuscation techniques" that scramble URLs so that, even in the event of a site compromise, additional records should not be easily accessible.

Lock\line spokesman Reed Garrett confirmed the hack. Carter noted that no financial information or social security number data were taken and the information wasn't even available to lock\line.

"We screwed up," said Carter. "Our policy is that any time there is a document with customer information on it is to be shredded. They've been trained on this. They just didn't do it. There's no excuse for it."

The event highlights the problems of managing vendor relationships when customer information needs to be shared but each company has different processes for handling that information. Carter says Cingular has nearly 40,000 vendors, and staying on top of them all is an "arduous" task, which the company continues to evaluate.

Jerry Brady, CTO of security services company Guardent, said incidents like the Cingular episode are not that uncommon.

"This usually happens because people whip together quick-and-dirty front ends without much thought to the construction of the data," he said. "You see this all the time, not just in the private sector, but in government systems as well. You just can't expect that outsourcer (to) treat confidential data the same way as the firm. They have no vested interest in worrying about the customer."

Lamo noted that outsourcing arrangements continue to yield a treasure trove of weak links in electronic security. Said Lamo, "As companies begin to outsource more and more of their businesses, the line of where security begins and ends gets blurry." He added that in this case, the security was "tremendously bad."

The Cingular discovery is the latest in a line of exploits from Lamo In the past few years, Lamo has found his way into the database containing sources for the *The New York Times,* has altered news stories on Yahoo and has repeatedly compromised AOL. Companies have contemplated suing him, but security experts have lauded his efforts for pointing out flaws.

Lamo, 22, doesn't have a permanent address. He wanders cross-country on foot or by public bus. Spring and summer usually bring him to Northern California. Until recently, he used terminals at Kinko's to perform his hacks. He has graduated to using a Wi-Fi-ready laptop at Starbucks to do his work.

For Lamo, there's a bigger issue at stake with the Cingular hack.

"If only they had recycled the document instead of throwing it away," he quipped, "this wouldn't have happened."

||||

FBI(19 cv 1495) 1809

To: [   ]
From: SA [   ]
Subject: Link to article
Cc:
Bcc:
Attached:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-11-2010 BY [   ] UC BAW/JK/RYS

bo 1,6
b7C 1,6

Hi, [   ]

It was a pleasure speaking with you today. Here is the link to the story I informed you of today.
Obviously this is an ongoing investigation so if you could be discrete about my calling you it would
be greatly appreciated. [   ]

I appreciate your assistance with this matter and if you ever need anything please let me know.

Thanks,

[   ]

Link: http://www.wired.com/news/privacy/0,1848,59024,00.html

b3 -1
b6 -1
b7C -1

bo 1
b7C 1

T-Mobile USA home

See all T-Mobile Interna

L 6   1
b 7C   1

··**T**··Mobile·HotSpot

Get more from

| Services | Locations | Sign Up | Support | Contact Us | Abo |

Services

- About the service
- ≫ Service Plans
- ≫ What you need
- ≫ Corporate accounts

Get More from Your Mobile Life.

T-Mobile HotSpot provides high-speed Wi-Fi wireless Internet access in public locations such as American Airlines Admirals Clubs, Starbucks coffeehouses and Borders Books & Music stores

This robust network is made for speed with a full T1 connection at every location Using either a PDA that is Wi-Fi 802.11b wirelessly-enabled, download your email attachments, watch a live w listen to streaming audio. Connect wirelessly, effortlessly to the world's largest public Wi-Fi netw

Right away, you'll see the benefits of a service that works to ensure a smooth connection to you and seamless integration with your existing Internet tools. What you won't see is a change in the service when you use it in different locations.

FAST - Connect to the Internet or your corporate intranet at blazing fast speeds - T-Mobile provides a full T1 connection to every location.

RELIABLE - Get the same high quality service in every location, giving you the peace of mind tl matter where you go, you'll experience the world class benefits of T-Mobile.

AFFORDABLE - Use it a little. Use it a lot Either way, there's a plan for you. Sign up for an unli monthly subscription plan starting at $29.95 or pay as you go for only $0.10 per minute

CONVENIENT - With T-Mobile HotSpot, there are no busy signals, no searching for phone jack of all, no waiting Connect easily, wirelessly, instantly.

⫸ Sign Up.

T-Mobile USA home

See all T-Mobile Interna

··**T**··Mobile·HotSpot

Get more from

| Services | Locations | Sign Up | Support | Contact Us | Abo |

Services

>> About the service

— Service Plans

>> What you need

>> Corporate accounts

Get More time in your day.

T-Mobile HotSpot offers a full line of service plans to meet the needs of any mobile user. Choos monthly subscription plans, a prepay option or a Pay as you go plan.

Plan Name	Price	Included Minutes	Add'l Minutes	Included Data Transfer	Other Information
Wi-Fi Subscription Plans For those who expect to connect regularly, we offer two unlimited Subscription plans.					
Unlimited National - Annual	$29.99 per month	Unlimited .	N/A	Unlimited	12 month contract required. Includes unlimited minutes and data at all service locations nationwide. Early termination fee of up to $200 ; You may terminate service without ; early termination fee if you cancel w first 30 days after plan commencem
Unlimited National - month to month	$39.99 per month	Unlimited	N/A	Unlimited	One month commitment required. Includes unlimited minutes and data at all service locations nationwide. An administrative fee of $25 applies terminations within the first 12 mont plan commencement. You may term service without paying an administra you cancel within the first 30 days a commencement.
Wi-Fi Prepay Plans Give the Wi-Fi service a try with a national, refillable prepay plan.					
Prepay 300	$50.00	300	300 minute refill is $50	Unlimited	No Minimum commitment. Sign-up and refill online at your con Minimum user session is 10 minute login
Wi-Fi Metered Plans If you expect to check email or download files only occasionally, try a pay as you go plan.					
Pay as you go	$0.10 per minute.	N/A	$0.10 per additional minute.	Unlimited	No term commitment. Minimum user session is 60 minute login. Use at any service location nationw

>> Sign Up

>> Additional terms and conditions apply, click here to see Rate Plan C·

If your laptop or handheld is already Wi-Fi 802 11b enabled, you can also sign up by simply lau your browser at thousands of HotSpot locations.

T-Mobile USA : ©2002-3 T-Mobile USA, Inc. : Terms of Use : Terms & Conditions : Privacy Policy : HotSpot Terms & Conditions : Hot!

T-Mobile International · Austria : Czech Republic : Germany : Netherlands : Poland . Russia : United Kingdom

🏴 T-Mobile USA home   See all T-Mobile Interna   b6 -1
                                              b7C -1

··T··Mobile·HotSpot   Get more from

| Services | Locations | Sign Up | Support | Contact Us | Abo |

Services

» About the service

» Service Plans

— What you need

» Corporate accounts

It's easy to get started.

Connecting to the T-Mobile HotSpot network is simple. Here's what you'll need:

1. A laptop, pocket PC or handheld device with Wi-Fi 802.11b wireless capability. Your existing device may already have this capability built-in. If not, you can purchase a Wi-Fi 802 11b wireless networking card for most laptops and many handhelds at any major electronics retailer.

Wireless Cards for Laptops

DLink Wireless LAN PC Card 11MBPS (DWL650)
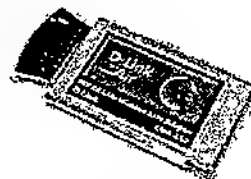
Netgear 11Mbs - 802.11b Wireless PC Card for Laptops

Featured Handheld Device

Sharp Zaurus SL-5500

Using a Wireless LAN Compact Flash card with your Zaurus will allow you to use Instant Messaging, email, the, Internet, and various other applications via the T-Mobile HotSpot network

Several CompactFlash cards are available from different manufacturers. Visit http://www.myzaurus com/buyaccess.asp for a complete list of cards you can use with the Zaurus.

Compact Flash cards

Netgear MA701 CompactFlash Card - 802.11b 11 Mbps w.reless card for handheld devices.

When your device is wireless-enabled, you will need to set your SSID (or network identifier) to 't Refer to your wireless network card documentation for specific instructions on how to make this or visit customer support.

2. Web Browser - You can use any standard Internet-ready browser on any operating system. I additional software is required

3. Service Plan - T-Mobile HotSpot has a full line of service plans to meet the needs of any mol

from small bundles of minutes for the occasional user to unlimited minutes of Internet access. S while you're here or launch your browser at any of our service locations and sign up for one of o plans.

Now you're ready to go. Visit any of the thousands of T-Mobile HotSpot service locations, launcl browser, log-in and you're connected. It's that simple.

If you have more questions on how to connect, we're here to help.

T-Mobile USA : ©2002-3 T-Mobile USA, Inc. : Terms of Use . Terms & Conditions : Privacy Policy . HotSpot Terms & Conditions . Hot!

T-Mobile International : Austria : Czech Republic · Germany : Netherlands : Poland : Russia · United Kingdom

06/12/2003
CAH:cah

     The attached article from Wired News, titled "Lamo Hacks Cingular Claims Site" was written on 5/29/2003 stating that ADRIAN LAMO has hacked CINGULAR using a T-Mobile hot spot at Starbucks.

     The attached information pertaining to T-Mobile hot spot services provided to STARBUCKS was obtained from t-mobile.com/hotspots. It states that an individual can either have a monthly account with T-mobile or a pay as you go account to utilize their hot spots throughout the country including STARBUCKS

     The attached email was sent to [ ] General Counsel, T-Mobile regarding the article in Wired News

b6 -1,5
b7C -1,5
b3 -2
b7E -3
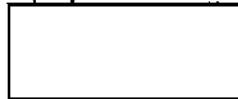
06/13/2003
CAH:cah

b3   2
b6   1
b7C   1
b7E   3

SA [ ] contacted [ ] Senate Legal Counsel, 642 Senate Hart Building, Washington, DC 20510 regarding the letter sent to their office on 5/13/2003 requesting information of the unauthorized intrusion of ADRIAN LAMO into senate.gov. [ ] stated that their technical people told her that [ ] I explained to [ ]

[ ] understood this concept and stated that I would have to speak to the technical people about this further.

b6 -1, 6
b7C -1, 6
b7E -1

[ ] further stated that her technical people did not like the term unauthorized intrusion used in the letter I sent to them   I explained to [ ] that in the article the Director of Technology, TRACY WILLIAMS stated that their proxy servers were misconfigured allowing access to individuals who were not authorized to use them   WILLIAMS stated the servers were taken off-line once this was discovered   I explained to [ ] that that is what is meant by unauthorized intrusion.

[ ] went on to explain that the hack of LAMO or anyone else into senate.gov is not important due to the fact that the computers do not hold pertinent information. I asked [ ] if it was the policy of www.senate.gov to allow hackers or anyone to gain full access to their proxy servers and web servers to use them, as they deem appropriate. She stated she was not sure if this was their policy and I would need to speak to the technical people about the policy.

[ ] explained that [ ] and that the technical people knew that it was an open proxy server that could be accessed by anyone and they were working on this problem. I asked her if they knew about the problem why were they not pulled off-line prior to the disclosure by LAMO. [ ] stated I would need to speak to the technical people regarding this matter

b6 -6
b7C -6
b7E -1

[ ] stated that she believed the technical people only spoke with the reporter and that no contact was made with LAMO directly. [ ] stated that she would make arrangements to have the technical people involved in this matter call me, when she had time.

email.wpd

UPLOADED
WITH/TEXT ✓
WITHOUT TEXT
BY
DATE JUN 2 4 2003

SERIALIZED   FILED

JUN 2 0 2003

b3 -2
bC -1
b7C -1
b7E -3

06/20/2003
CAH:cah

On 6/20/2003, SA [ ] received the attached email from [ ] from SBC, Inc   The email contained files pertaining to the hack of ADRIAN LAMO of SBC.

Copies will be maintained in the file.

b6   1,2
b7C   1,2
b7   2
b7E   3

To: "'SA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE ... ...

Finally got everything approved to release information on the Lamo Case to
you. The attached files should be helpful. If you have questions please
let me know.

Per your request here is my address.

b6 -1,2
b7C -1,2
b7E -1

2600 N. Central Expressway
Suite 528
Richardson TX. 75080

Thanks

Corporate Information Security

b6 -1,2
b7C -1,2
b7E -1

bigid1.wpd

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 07/08/03 Time: 08:53

Case ID: [   ]

Description of Document:

    Type : INSERT
    Date : 07/07/03
    To   : NEW YORK
    From : NEW YORK
    Topic: CHECKS ON 81 INDIVIDUALS W/ATTACHED RESULTS

b3 -2
b6 -1
b7C -1
b7E -3

Reason for Permanent Charge-Out:

    inadvertently uploaded

Transferred to:

    Case ID: [   ]
    Employee: [   ]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 07/18/2003

To: New York   **Attn:** SA ☐

From: Cincinnati
         Squad 4/Columbus RA
         Contact: SA ☐

Approved By: ☐

Drafted By: ☐ rew

Case ID #: ☐

b3 -2
b6 -1
b7C -1
b7E -3

Title: ADRIAN LAMO;
        New York Times-Victim;
        Computer Intrusion;
        OO:NY

Synopsis: To respond to lead set by New York.

Reference: ☐

Details: Vincent Glaze died on 09/03/1998. He is interred
alongside his wife, Dorothy S. Glaze, at Huntsville Cemetery
McArthur Township, 3691 Road 37 West, Huntsville, OH, 43324,
(937)686-2766.

        Cincinnati considers lead covered.

b3 -2
b7E -3

LEAD(s):

Set Lead 1:   (Info)

    NEW YORK

        AT NEW YORK, NY

        For information only.

♦♦

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 79
Page 43 ~ Duplicate;
Page 44 ~ Duplicate;
Page 45 ~ Duplicate;
Page 46 ~ Duplicate;
Page 47 ~ Duplicate;
Page 48 ~ Duplicate;
Page 49 ~ Duplicate;
Page 50 ~ Duplicate;
Page 51 ~ Duplicate;
Page 52 ~ Duplicate;
Page 53 ~ Duplicate;
Page 54 ~ Duplicate;
Page 56 ~ Duplicate;
Page 57 ~ Duplicate;
Page 58 ~ Duplicate;
Page 59 ~ Duplicate;
Page 60 ~ Duplicate;
Page 61 ~ Duplicate;
Page 62 ~ Duplicate;
Page 63 ~ Duplicate;
Page 64 ~ Duplicate;
Page 65 ~ Duplicate;
Page 66 ~ Duplicate;
Page 67 ~ Duplicate;
Page 68 ~ Duplicate;
Page 69 ~ Duplicate;
Page 70 ~ Duplicate;
Page 71 ~ Duplicate;
Page 72 ~ Duplicate;
Page 73 ~ Duplicate;
Page 74 ~ Duplicate;
Page 75 ~ Duplicate;
Page 76 ~ Duplicate;
Page 77 ~ Duplicate;
Page 78 ~ Duplicate;
Page 79 ~ Duplicate;
Page 80 ~ Duplicate;
Page 81 ~ Duplicate;
Page 82 ~ Duplicate;
Page 83 ~ Duplicate;
Page 84 ~ Duplicate;
Page 85 ~ Duplicate;
Page 86 ~ Duplicate;
Page 87 ~ Duplicate;
Page 88 ~ Duplicate;
Page 89 ~ Duplicate;
Page 90 ~ Duplicate;
Page 91 ~ Duplicate;

```
Page 92 ~ Duplicate;
Page 93 ~ Duplicate;
Page 94 ~ Duplicate;
Page 95 ~ Duplicate;
Page 96 ~ Duplicate;
Page 97 ~ Duplicate;
Page 98 ~ Duplicate;
Page 99 ~ Duplicate;
Page 100 ~ Duplicate;
Page 101 ~ Duplicate;
Page 102 ~ Duplicate;
Page 103 ~ Duplicate;
Page 104 ~ Duplicate;
Page 105 ~ Duplicate;
Page 106 ~ Duplicate;
Page 107 ~ Duplicate;
Page 108 ~ Duplicate;
Page 109 ~ Duplicate;
Page 110 ~ Duplicate;
Page 111 ~ Duplicate;
Page 112 ~ Duplicate;
Page 113 ~ Duplicate;
Page 114 ~ Duplicate;
Page 115 ~ Duplicate;
Page 116 ~ Duplicate;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 119 ~ Duplicate;
Page 120 ~ Duplicate;
Page 121 ~ Duplicate;
Page 122 ~ Duplicate;
```

```
XXXXXXXXXXXXXXXXXXXXXXXX
X    Deleted Page(s)     X
X    No Duplication Fee X
X    For this Page       X
XXXXXXXXXXXXXXXXXXXXXXXX
```

| Home | The Basics | Microsoft | UNIX | IDS | Incidents | Virus | Pen-Test | Firewalls | Bugtraq |

*: Vulnerabilities   *: Library   *: Calendar   *: Tools   *: Service Vendors   *:* Free Analyzer Download

<< Printable version >>

SECURITYFOCUS NEWS

Adrian Lamo charged with computer crimes

By *Kevin Poulsen*, SecurityFocus Sep 5 2003 10:11AM

FBI agents armed with a federal arrest warrant out of New York were searching for Adrian Lamo Thursday, SecurityFocus has confirmed.

Lamo has been charged in New York under Title 18 U.S.C. 1030 and 1029, according to deputy federal public defender Mary French, who says she's spoken with one of the FBI agents that were searching for Lamo. The federal laws prohibit unauthorized access to a protected computer, and illegal possession of stolen "access devices" -- a term that encompasses passwords, credit card numbers, and the like. French did not know what the specific allegations were, because the charging document is sealed.

Two agents visited the home of Lamo's parents, Mario and Mary Lamo, near Sacramento, California, Thursday afternoon, Mary Lamo said Thursday. "They wouldn't tell us anything but that they had an arrest warrant and they wanted to come in," she adds.

When she demurred, the agents vowed to return with a search warrant, then began overtly watching the house from parked cars, she said. "They followed me when I went out, so they're not hiding it."

Friday morning, a spokesperson for the U.S. Attorney's office in New York confirmed that the office had an open case file on Lamo, but otherwise declined to comment.

Lamo frequently stays at his parents' home, but he was not there at the time of the FBI's visit, and has not returned since. His mother contacted the Federal Public Defender's office in Sacramento, which has agreed to handle his surrender.

> **'I have always said that actions have consequences, and this is something that I was always aware might happen.'**
> -- Adrian Lamo

"If he's arrested or turns himself in in this district, we will represent him for the initial proceedings," French said Friday morning. "I haven't had any direct contact with him yet."

In a telephone interview Thursday, Lamo said he was in California, but did not plan to turn himself in until after conferring with the attorney. The hacker was quick-witted and seemingly in good humor, with only a trace of nervousness in his voice. He quipped about the proper etiquette of being arrested by the FBI, and suggested jokingly that SecurityFocus should purchase the publication rights to a favorite photo. He said he was in the

company of a camera crew producing a television documentary on hackers.

"I have always said that actions have consequences, and this is something that I was always aware might happen," said Lamo. "I don't intend to deny anything that I have done, but I do intend to defend myself vigorously."

The 22-year-old Lamo has become famous for publicly exposing gaping security holes at large corporations, then voluntarily helping the companies fix the vulnerabilities he exploited -- sometimes visiting their offices or signing non-disclosure agreements in the process.

Until now, his cooperation and transparency have kept him from being prosecuted. Lamo's hacked Excite@Home, Yahoo, Blogger, and other companies, usually using nothing more than an ordinary Web browser. Some companies have even professed gratitude for his efforts: In December, 2001, Lamo was praised by communications giant WorldCom after he discovered, then helped close, security holes in their intranet that threatened to expose the private networks of Bank of America, CitiCorp, JP Morgan, and others.

Lamo believes the arrest warrant is for his most high-profile hack. Early last year he penetrated the *New York Times*, after a two-minute scan turned up seven misconfigured proxy servers acting as doorways between the public Internet and the *Times* private intranet, making the latter accessible to anyone capable of properly configuring their Web browser.

MORE FROM SECURITY FOCUS...

RELATED STORIES
- Panel Debates Hacker Amnesty
- New York Times Internal Network Hacked
- Who Is Adrian Lamo?
- Yahoo! News Hacked
- Proxy Exposes Excite@Home Data

Once inside, Lamo exploited weaknesses in the *Times* password policies to broaden his access, eventually browsing such disparate information as the names and Social Security numbers of the paper's employees, logs of home delivery customers' stop and start orders, instructions and computer dial-ups for stringers to file stories, lists of contacts used by the Metro and Business desks, and the "WireWatch" keywords particular reporters had selected for monitoring wire services.

He also accessed a database of 3,000 contributors to the *Times* op-ed page, containing such information as the social security numbers for former U.N. weapons inspector Richard Butler, Democratic operative James Carville, ex-NSA chief Bobby Inman, Nannygate veteran Zoe Baird, former secretary of state James Baker, Internet policy thinker Larry Lessig, and thespian activist Robert Redford. Entries with home telephone numbers include Lawrence Walsh, William F. Buckley Jr., Jeanne Kirkpatrick, Rush Limbaugh, Vint Cerf, Warren Beatty and former president Jimmy Carter.

In February, 2002, Lamo told the *Times* of their vulnerability through a SecurityFocus reporter. But this time, no one was grateful, and by May federal prosecutors in New York had begun an investigation.

"I think this is unsporting of the New York Times," Lamo said Thursday.

Lamo's mother said she has no opinion on her son's exploits. She's just worried about him.

"I don't really know much of anything about computers," says Mary Lamo. "He's my son. Right now, all I can worry about is how I can help him."

"I hope there will be a time when Adrian can do positive things that everyone agrees are positive," she adds.

<tips@securityfocus.com>
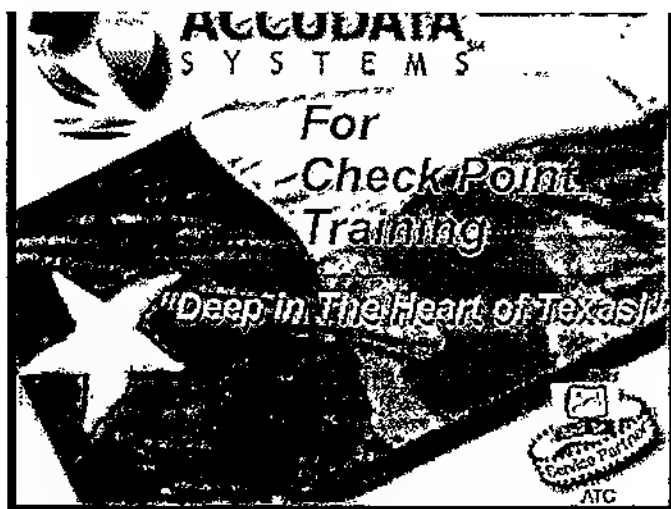
Discussion
don't look back remo williams
   don't look back Anonymous
      don't look back Anonymous
FBI reportedly hunting Adrian Lamo Dr. Lin
   degrees of seperation Anonymous
      degrees of seperation Anonymous
      degrees of seperation Anonymous
      degrees of seperation Anonymous
      degrees of seperation bobcov
         degrees of seperation Sunfire
FBI reportedly hunting Adrian Lamo Anonymous
FBI reportedly hunting Adrian Lamo The 420 Zodiac
FBI reportedly hunting Adrian Lamo Anonymous
   New Instructions for Reporting Holes dyc0n@mchsi.com
      New Instructions for Reporting Holes Anonymous
      New Instructions for Reporting Holes bobcov
NYT lusers Citizen Caned
FBI reportedly hunting Adrian Lamo Anonymous
   FBI reportedly hunting Adrian Lamo Anonymous
      FBI reportedly hunting Adrian Lamo Anonymous
         FBI reportedly hunting Adrian Lamo Anonymous
            FBI reportedly hunting Adrian Lamo ab
FBI reportedly hunting Adrian Lamo Anonymous
   FBI reportedly hunting Adrian Lamo eGod
   FBI reportedly hunting Adrian Lamo Anonymous
   FBI reportedly hunting Adrian Lamo Anonymous
   FBI reportedly hunting Adrian Lamo Anonymous
Adrian Lamo charged with computer crimes Anonymous
   Adrian Lamo charged with computer crimes Anonymous
   Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Option SoCal
blah Anonymous
   blah Anonymous
      blah Anonymous

blah Lic
blah ferretzero
blah ferretzero
blah Anonymous
blah history repeats
blah bobcov
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Zack Wilson
Adrian Lamo charged with computer crimes ferretzero
Good luck SilverStar
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes _cHiCkEn
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Poor Guy Keepr
Poor Guy Anonymous
Adrian Lamo charged with computer crimes Anonymous
Objective View dvhart
Objective View Puerto_Rocco
Adrian Lamo charged with computer crimes GreyGeek
First false stories, then shoot the messenger cpopin
First false stories, then shoot the messenger Anonymous
First false stories, then shoot the messenger Anonymous
THINK ?
THINK Anonymous
THINK Anonymous
THINK Anonymous
THINK Anonymous
THINK Anonymous
THINK Anonymous
THINK Anonymous
THINK dijjnn
More ?
Malpractice Anonymous
Malpractice ferretzero
THINK Anonymous
THINK junktext
Adrian Lamo charged with computer crimes Anonymous
The control mechanisms of the ignorant Anonymous
Dumb Americans Jean Pierre Rupp
Dumb Americans Anonymous
Dumb Americans Anonymous
Blind Americans...but not dumb. Anonymous
World-wide police Anonymous
this is not right jfrances@mcintoshstudent.com
this is not right Anonymous
Adrian Lamo charged with computer crimes konsole
Adrian Lamo charged with computer crimes Anonymous
Companies that he helped should now help him Anonymous
Some free advice for Adrian (the lawyers will charge :-) Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes Anonymous
Adrian Lamo charged with computer crimes mace
Adrian Lamo charged with computer crimes The IMF

Adrian Lamo charged with computer crimes   ferretzero
Adrian Lamo charged with computer crimes   Anonymous
Heh...he was in Sacramento 2 days ago.   Ericka
     Heh...he was in Sacramento 2 days ago.   Anonymous
       Heh...he was in Sacramento 2 days ago.   Ericka
Too Far?   jelo
not another mitnick trial   Anonymous
Adrian Lamo charged with computer crimes   Anonymous
DON'T BECOME A FUGITIVE FROM INJUSTICE, TURN YOURSELF IN NOW.   Anonymous
Adrian Lamo charged with computer crimes   Anonymous
No good deed goes unpunished ...   Anonymous
keep on truckin my friend   mick_nobody
Adrian Lamo charged with computer crimes   digital reciever
Adrian Lamo charged with computer crimes   Blah
Adrian Lamo charged with computer crimes   Anonymous
Adrian Lamo charged with computer crimes   .Net³
     Playing nice might get you busted   Anonymous
Adrian Lamo just showed them how easy it is   Bernout13
Adrian Lamo charged with computer crimes   Anonymous
Adrian Lamo charged with computer crimes   ICAMACHO

[Post a comment]

FBI(19-cv-1495)-1892

| Slashdot ▼ | | Search | \ |

Slashdot
News for Nerds. Stuff that matters.

Adrian Lamo Charged With Hacking

Posted by Cowboy Neal on Saturday September 06, @10:41AM
from the high-profile-hacking dept.

retro128 writes *"Drifting around the US from state-to-state, Adrian Lamo has been making news for some time with his 'White Hat' hacking exploits His highest-profile hacking has included Excite@Home and Yahoo After he would break into a network, he would call up those in charge of it and help them fix the holes So far, it has earned him praise from the administrators of those systems, but now SecurityFocus is carrying the story that the FBI has filed charges against him, and currently has his parents' house staked out The records are sealed, so nobody knows who is responsible, but Lamo suspects the New York Times initiated the investigation when they found out how deep into their system he got "*

< Bruce Schneier on Security Tradeoffs FCC Ponders Removing Morse Code Reqs for Amateur Radio Licenses >

Index Only | Search Discussion

Threshold: | 1: 353 comments ▼ | | Threaded ▼ | | Oldest First ▼ |

[Change] [Reply]

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

(1) | 2

- <u>Fit? Stops. R</u> by Anonymous Coward (Score:2) Saturday September 06, @10:43AM

  - <u>Re:Fit? Stops. R</u> by Anonymous Coward (Score:1) Saturday September 06, @04:15PM
  - <u>Re:Fit? Stops. R</u> by jbottero (Score:1) Sunday September 07, @01:33AM
    - o <u>Re:Fit? Stops. R</u> by krymsin01 (Score:3) Sunday September 07, @02:26AM
      - ▪ <u>Re:Fit? Stops. R</u> by zootread (Score:2) Sunday September 07, @10:12AM
      - ▪ <u>Re:Fit? Stops. R</u> by zootread (Score:2) Sunday September 07, @10:24AM
    - o **1 reply** beneath your current threshold.

The Real Problem (Score:5, Funny)
by <u>Goo.cc (687626)</u> * <jeff@goo.cc> on Saturday September 06, @10:43AM (#6887104)
(http://goo.cc/)

Maybe the real problem that the New York Times has with Lamo is that he was able to read stories without having to register for a free account. (Hell, that stupid registration requirement make me want to hack them too.)

[Reply to This]

    Re:The Real Problem (Score:5, Funny)
    by <u>Surak (18578)</u> * <surak@mailblHORS ... minus herbivore> on Saturday September 06, @10:47AM (#6887125)
    (http://colonialfamilies.com/ | Last Journal: Thursday September 04, @03.14PM)

    Yep. That whole &partner=GOOGLE thing will get the FBI after ya. Watch out!
    [Reply to This | Parent]

- o <u>Re:The Real Problem</u> by Anonymous Coward (Score:2) Saturday September 06, @11:40AM
- o <u>Re:The Real Problem</u> by shfted! (Score:3) Saturday September 06, @01:01PM
- o <u>Re:The Real Problem</u> by crucini (Score:2) Sunday September 07, @01:44AM

- <u>Re:The Real Problem</u> by Anonymous Coward (Score:1) Saturday September 06, @10:48AM
- <u>Re:The Real Problem</u> by SunPin (Score:2) Saturday September 06, @11.11AM

    Re:The Real Problem (Score:5, Informative)
    by <u>FsG (648587)</u> <'ten.ecivrestob' 'ta' 'gsf'> on Saturday September 06, @11:33AM (#6887374)
    (http://fsg.botservice.net/)

    No need to look for new exploits when the existing ones suffice..
    1. Click on URL, you're redirected to registration/login page
    2. Go to URL bar, replace "www" with "archive" in the URL, leaving the rest alone, and hit ENTER
    3. The system will bounce you around a few erroneous URLs, before returning you to the homepage
    4. All NYT links will now work without registration, thanks to a special cookie

4. All NYT links will now work without registration, thanks to a special cookie set by the bouncing process

[Reply to This | Parent]

- o Re:The Real Problem by twofidyKidd (Score:1) Saturday September 06, @01:29PM
- o Re:The Real Problem by Anonymous Coward (Score:1) Saturday September 06, @02:50PM
- o Re:The Real Problem by dmuth (Score:2) Saturday September 06, @06.07PM
- o **2 replies beneath your current threshold.**
- Re:The Real Problem by Anonymous Coward (Score:2) Saturday September 06, @11 34AM
- Re:The Real Problem by Anonymous Coward (Score:1) Saturday September 06, @12.52PM
  - o **1 reply beneath your current threshold.**
- Re:The Real Problem by Digitalexikon (Score:1) Saturday September 06, @04.17PM
- Re:The Real Problem by CodeGorilla (Score:1) Saturday September 06, @07:32PM
- Hack the NYTIMES?! by Safety Cap (Score:2) Saturday September 06, @10:21PM

- And good riddance. by JeffTL (Score:3) Saturday September 06, @10.46AM

Re:And good riddance. (Score:5, Insightful)
by SerpentDrago (703376) * on Saturday September 06, @10:52AM (#6887138)

If you ask and tell theam your going to try to hack. Then they will tighten security. Thats exactly why you can't tell theam. You have to just do it. at a random time without theam knowing , then see if they catch it. Thats the only true way to "test" Do it Blind or it is not real. A BlackHat will never ask or tell you when.

[Reply to This | Parent]

- o Re:And good riddance. by the_2nd_coming (Score:1) Saturday September 06, @11:34AM

Re:And good riddance. (Score:5, Insightful)
by Shoten (260439) on Saturday September 06, @11:46AM (#6887427)

I think you're confusing what Lamo did with something that the NYT actually gave permission for. I agree with you, that a penetration test should be performed in such a way as to be unexpected, so paranoid admins can't do stupid things to improve the results (like turn off all inbound access for a day). But this wasn't a penetration test, it was nothing more than an uninvited and deeply illegal intrusion plus some spin control for the media.

I know a lot of people look at it and say, "Oh, but he had good intentions, that makes it ok!" It's not really like that...we don't KNOW his real intentions at all, just what he SAYS his intentions are. But, if someone owned your network, would you just trust them when they say they didn't do anything more insidious than they told you about? I wouldn't, and the resulting cleanup to make sure that nothing more was done is an expensive and disruptive process. This is part of why the damages for relatively minor hacks end up being so enormous in many cases.

We're always pushing ourselves to question what we're being told by the media, by our leaders, by our educators, by big business...we should really question anyone who might have an ulterior motive.

[Reply to This | Parent]

- Re: hacking and intentions.... by King_TJ (Score:2) Saturday September 06, @01·28PM
    - Re: hacking and intentions.... by parliboy (Score:3) Saturday September 06, @03.00PM
    - Re: hacking and intentions.... by Quothz (Score:3) Saturday September 06, @06:39PM
    - Re: hacking and intentions.... by Tadghe (Score:3) Saturday September 06, @08:19PM
    - Re: hacking and intentions.... by RancidBeef (Score:1) Saturday September 06, @08:54PM
        - Re: hacking and intentions.... by aricusmaximus (Score.1) Saturday September 06, @11:36PM
    - 1 reply beneath your current threshold.
- Re:And good riddance. by frater_corvus (Score:2) Saturday September 06, @09:34PM
- 3 replies beneath your current threshold.

Good intentions don't mean it is legal (Score:5, Insightful)
by rblancarte (213492) on Saturday September 06, @11:50AM (#6887448)
(http://www.blancarte com/ron | Last Journal: Thursday January 23, @11:31PM)

Drago - you are a fool. If you are hacking people's systems without their permission, YOU ARE BREAKING THE LAW. PERIOD. END OF STORY. If people were allowed to say "Well, I was doing it so I could help their security", then you would have all sorts of Blackhats hacking systems, and then claiming, "I was going to help, but you arrested me first." No.

Look, there are ways to do security checks like this, without the security teams knowing that you are doing it. Get permission, make sure that no one is tipped off, and then test the systems.

If there is one thing I can't stand it is people doing illegal actions and then claiming they are doing it for the greater good. This type of action cannot be condoned. Sure, you might be doing help, but you also might not.

[Reply to This | Parent]

- Re:Good intentions don't mean it is legal by rwise2112 (Score:1) Saturday September 06, @12:52PM
- Re:Good intentions don't mean it is legal by ThePorkHawke (Score:1) Saturday September 06, @01:13PM
    - Re:Good intentions don't mean it is legal by rikkards (Score:2) Saturday September 06, @01:27PM
        - Re:Good intentions don't mean it is legal by MoneyT (Score:2) Saturday September 06, @01.30PM
            - Re:Good intentions don't mean it is legal by rikkards (Score:2) Saturday September 06, @03:21PM
        - Re:Good intentions don't mean it is legal by staticdragon (Score:1) Saturday September 06, @02:51PM

(Score:1) Saturday September 06, @02:31PM

Re:Good intentions don't mean it is legal (Score:4, Funny)
by Kenja (541830) on Saturday September 06, @03:00PM
(#6888534)
(http://www.klassy.com/)

If the post man goes into your house, rumages around and then leaves you a note that your underwear is dirty and your out of milk he should be arested.

[Reply to This | Parent]

- Re:Good intentions don't mean it is legal by 1lus10n (Score·2) Saturday September 06, @06:41PM
- **1 reply** beneath your current threshold.

- Re:Good intentions don't mean it is legal by FussionMan (Score:1) Saturday September 06, @01:55PM

Re:Good intentions don't mean it is legal (Score:5, Insightful)
by Izago909 (637084) on Saturday September 06, @02:59PM
(#6888530)

So let's throw the (relatively) most desirable type of hacker in jail so he gets out of the way of the black hats. This is some bullshit logic. Regardless of what his 'true' intentions were, his track record speaks volumes: He's always come clean with people.

While network admins are busy giving themselves kudos for integrating Microsoft's latest and greatest secure systems, he is busy looking for holes. Without these types of white hats, all the world would have is insecure networks remaining open to black hats until they discovered the holes the really hard way.

Screw all the evil, sinister things you think his 'true' intentions are. He and his counterparts have potentially saved your company millions in expenses when some black hat could have made off with gigabytes of confidential data. Think these white hats are bad? Wait until you have class actions out the wazoo because many of your customers are now facing the business end of your over confidence. Screw modern hacking laws because they are stale and outdated. People always like to tack on new laws without even considering removing or revising obsolete sections. All it's going to do is alienate any potential allies. The bad guys won't get caught because they hide, the good guys don't hide because they think they don't have a reason to.

White hats are thrown in jail because they get bad attention and can cause a PR mess. Many times, the work of black hats can be covered up by the company or government. How many stories have we heard of hackers holding sensitive data ransom or extorting businesses in some way? You really don't think EVERY incident gets publicized, do you? These people want to make it look like they are tough on hackers, so they go after the easiest and most public targets.

You will be giving a powerful message to upcoming generations of hackers. If the end result is the same, what the hell do I need this white hat for?

Someone **will** come knocking at your door, it's inevitable. What

color of this ~~illegible~~ at your door, it's inevitable. What color hat do you want him to be wearing?

[Reply to This | Parent]

- Re:Good intentions don't mean it is legal by putaro (Score:2) Saturday September 06, @11:22PM
  - Re:Good intentions don't mean it is legal by Izago909 (Score:2) Sunday September 07, @04:47AM
  - 1 reply beneath your current threshold.
- Re:Good intentions don't mean it is legal by arose (Score 2) Saturday September 06, @03:39PM
  - 2 replies beneath your current threshold.
  o Re:And good riddance. by HidingMyName (Score:3) Saturday September 06, @02:59PM
    - Re:And good riddance. by HidingMyName (Score:2) Saturday September 06, @07:45PM
      - Re:And good riddance. by HidingMyName (Score:2) Sunday September 07, @02:13PM
      - 1 reply beneath your current threshold.
    - 1 reply beneath your current threshold.

Re:And good riddance. (Score:4, Insightful)
by xplenumx (703804) on Saturday September 06, @05:27PM (#6889410)

The University of Washington had a "student run" program where returning students could volunteer to help freshmen move into their dorm room. In return for their help, the UW would supply the volunteers with free food (Usually through SubWay, Dominos, etc, with a student leader ordering the food using UW budget codes). After everyone moved in, the group would disband and everyone would forget about it until the following fall. Approximately six years ago, the student leader who was in charge of ordering food decided in Winter quarter that he would use the budget codes and try to order up some food for him and his friends (http://tinyurl.com/mhck) . What was Eric's excuse when he was eventually caught? "I was just trying to show how insecure the system was" and "I was really doing Res. Life a favor". Sound familiar? Eric Feigenbaum then wrote a series of articles to the student newspaper, The Daily, regarding his experience and how the university didn't appreciate his 'generous act'. Personally I become extremely nervous when someone decides to conduct some unannounced public service, especially through illegal means. Usually the "I'm just misunderstood. I was really trying to help out" excuse comes out after the individual gets caught, but some individuals will come forward first, hoping that it'll cover their tracks. For example, I had one employee to came up to me and said that they learned how to use the copier without first putting in their copy code. Turns out the employee decided to "test" his method by making over 5000 copies over a period of three days (all after hours). Another employee within the firm reported that some equipment was missing (it would have been discovered later that week). It was eventually discovered that the very same employee had stolen the equipment the night before. I don't know the first thing about Adrian Lamo besides what's written in the referenced article. He may be the most honest, altruistic, and generally nice guy in the world. Good for him. The problem is that the next Adrian Lamo may not

world. Good for him. The problem is that the next Adrian Lamo may not
be.

[Reply to This | Parent]

- Re:And good riddance. by Planx_Constant (Score:1) Saturday September 06, @07:49PM
  o 1 reply beneath your current threshold.
- Re:And good riddance. by arose (Score:2) Saturday September 06, @03:32PM
  o Re:And good riddance. by JeffTL (Score:1) Saturday September 06, @09:38PM

- Great Excuse by Pave Low (Score:3) Saturday September 06, @10:48AM

  - Re:Great Excuse by UWC (Score:1) Saturday September 06, @10:53AM
    o Re:Great Excuse by alienw (Score:2) Saturday September 06, @11:04AM

      Horrible analogy. (Score:5, Insightful)
      by pb (1020) on Saturday September 06, @11:08AM (#6887234)
      What if I just leave a signed note on the inside of your car that says
      "follow these three easy steps, and then no one else will be able to
      break into your car again"? Do you say "hey, thanks, buddy!", or
      "hey, someone broke into my car!"...
      [Reply to This | Parent]

        Response (Score:4, Insightful)
        by Overly Critical Guy (663429) on Saturday September 06,
        @12:08PM (#6887586)
        (Last Journal: Sunday August 10, @10:26PM)
        I say, "Why did you have to break into my car to write me a
        note?"
        [Reply to This | Parent]

          - How else... by idontneedanickname (Score:2) Saturday
            September 06, @01:05PM
            - Re:How else... by Nept (Score:2) Saturday September
              06, @04:29PM
            - Because... by idontneedanickname (Score:2)
              Saturday September 06, @06:42PM
            - Re:Because... by Nept (Score:2) Saturday September
              06, @08:07PM
            - Sorry, I misunderstood by idontneedanickname
              (Score:1) Saturday September 06, @10:49PM
          - 1 reply beneath your current threshold.
          - Re:Horrible analogy. by Sycraft-fu (Score:3) Saturday September
            06, @12:12PM
            - Re:Horrible analogy. by irc.goatse.cx troll (Score:2)
              Saturday September 06, @03:54PM
              - And? by Sycraft-fu (Score:2) Sunday September 07,
                @05:17AM
            - 1 reply beneath your current threshold.
          - Re:Horrible analogy. by Art Tatum (Score:1) Saturday September
            06, @12:50PM
          - Re:Horrible analogy. by Just Some Guy (Score:2) Saturday
            September 06, @02:02PM
          - Re:Horrible analogy. by WhaDaYaKnow (Score:2) Saturday
            September 06, @02:08PM

- **1 reply** beneath your current threshold.

Re:Great Excuse (Score:5, Insightful)
by pantropik (604178) on Saturday September 06, @11:21AM
(#6887307)

That's a really awful analogy.

If someone steals your car they are doing you a serious disservice and actively depriving you of something you cannot easily do without.

To use your analogy in a way that actually makes sense:

He isn't stealing your car. He is walking up and seeing if the door is unlocked and the keys are in the ignition. At the very MOST he is starting the car to prove he COULD steal it if he wanted to. But he never actually steals the car or harms you in any way (except maybe making you feel really stupid for having such an easily stolen car). He doesn't deprive you of it "for a month".

Basically he's checking to see if he COULD steal your car, NOT stealing it. Then he tells you what to do to keep others from stealing it.

Doesn't sound like evil incarnate to me. If I was being a total idiot as regards security I think I'd appreciate it if someone pointed that out to me before someone else came along and took advantage of it and ended up doing real harm.

The shame would be worth it in the end, I think. Unless you happen to be the NY Times, which is probably pretty sick of being shamed at this point.

[Reply to This | Parent]

- Re:Great Excuse by Anonymous Coward (Score:1) Saturday September 06, @11:51AM
    - **1 reply** beneath your current threshold.
- Re:Great Excuse by rblancarte (Score:2) Saturday September 06, @11:58AM

    Re:Great Excuse (Score:5, Funny)
    by Shanep (68243) on Saturday September 06, @12:22PM (#6887653)
    (http://slashdot.org/)

    YOU CANNOT BREAK THE LAW, EVEN FOR GOOD REASONS! IF YOU DO, EXPECT TO GO TO JAIL!

    I would bust his skull open with my tire iron, then call the cops.

    Okay, so busting this guys skull open is breaking the law for:

a) A good reason.
b) A bad reason.
c) No reason at all.
d) None of the above.

BTW, the thief will sue you from here to eternity.
Maybe if you make it out of jail alive some day, you
might be able to find a job to pay off that lifetime of
debt to him.

;)

You can't just go around breaking open skulls because
someone pisses you off. YOU CANNOT BREAK THE
LAW, EVEN FOR GOOD REASONS! IF YOU DO,
EXPECT TO GO TO JAIL!

[Reply to This Parent]

- Re:Great Excuse by Planx_Constant (Score.1) Saturday
  September 06, @07:58PM
- Re:Great Excuse by Angram (Score:2) Saturday September 06,
  @12:14PM
- Re:Great Excuse by shepd (Score:1) Saturday September 06,
  @12:40PM

Re:Great Excuse (Score:5, Insightful)
by arth1 (260657) on Saturday September 06, @01:07PM
(#6887895)
(http://2130706433/)

What companies do about those who warn them is what irks
me. Not only do they press charges as if they had been
maliciously broken into, but they tend to want to bill the
white hat hacker for EVERYTHING related to the incident,
including but not limited to ignorant PHBs spending months
in meetings about it, as well as the price for fixing the mess.

It's like you getting to work one day and finding a note stating
"the bathroom window opens from the outside, and the spare
key for the filing cabinet where you keep customer data
shouldn't be taped to the bottom of the counter." Then what
do you do? Call in all the staff, and close up the store for a
week while you hold meetings, followed by changing all the
locks and buying a gun, and finally suing the person who left
the note, charging him with the total costs of what you did?

Or you tell a farmer that you were hiking in his woods when
you discovered that his game warden was poaching. The
farmer's reaction is charging you with trespassing. While he
may have a legal right to do so, he'd be a real jerk AND idiot
to do so

The above is, unforunately, the analog to what's happening in the electronic world.

I'm not saying that Lamos and other self-appointed white hat hackers are RIGHT in what they do (I believe they aren't), but even if the messenger isn't welcome, you don't shoot him or blame hime for all the problems he reports.
The main reason why you shouldn't do that isn't just because it's a petty thing to do, but because you HURT yourself and others in the long run.

See, if I were a hacker operating like Lamos, and saw companies doing that, instead of alerting the companies and risking facing their and the paranoid law makers full wrath, I would stop alerting the companies about their flaws -- instead, I would anonymously alert the PUBLIC.

Seen from the viewpoint of a company, what's better about that? Yet, that's what they're pushing hackers into.
The companies might argue that they would want people to stop rattling doors in the first place, and that's a valid argument. However, it's not going to happen until you have exterminated every potential criminal and curious kid on the planet.
In a Utopia, you don't even need a door lock, because no-one would ever walk through the door without a right to do so. However, companies can't argue that as a defense -- not installing a lock would be seen as gross negligence, because it's **expected** that criminals and curious people **will** trespass unless minimal safety measures are taken. That's how our society is.

Charging Lamos is a signal, all right. Unfortunately the signal isn't "don't test our security uninvited", but "once you've tested our security uninvited, don't tell us -- stay anonymous and tell it to everyone else".

Regards,
--
*Art

[Reply to This | Parent]

- Re:Great Excuse by Penguin's Advocate (Score:2) Saturday September 06, @04:30PM
- Re:Great Excuse by Shdwdrgn (Score:1) Sunday September 07, @01:50PM
- Re:Great Excuse by iserlohn (Score:1) Saturday September 06, @01:17PM
- Re: the car analogy by King_TJ (Score:2) Saturday September 06, @01:38PM

- Re: the car analogy by Mordanthanus (Score:1) Saturday September 06, @07:48PM
- Re: the car analogy by King_TJ (Score:2) Sunday September 07, @12·48PM
- 1 reply beneath your current threshold.
- Re:Great Excuse by Just Some Guy (Score:2) Saturday September 06, @02:07PM
  - Re:Great Excuse by Just Some Guy (Score:2) Saturday September 06, @02:54PM
    - Re:Great Excuse by arose (Score:2) Saturday September 06, @03:52PM
      - Re:Great Excuse by Just Some Guy (Score:2) Saturday September 06, @04:01PM
        - Re:Great Excuse by arose (Score·2) Saturday September 06, @04.09PM
          - Re:Great Excuse by Just Some Guy (Score.2) Saturday September 06, @04:15PM
            - Re:Great Excuse by arose (Score·2) Saturday September 06, @04:22PM
    - 2 replies beneath your current threshold.
  - Re:Great Excuse by WhaDaYaKnow (Score·2) Saturday September 06, @02:31PM
    - 1 reply beneath your current threshold.
  - 1 reply beneath your current threshold.

Re:Great Excuse (Score:4, Insightful)
by xenoandroid (696729) on Saturday September 06, @11:21AM (#6887310)
(http://www.xenouniverse.com/)

The difference is that he didn't hijack the servers and use them for his own deeds for a month and returned them. He got in, observed how severe the exploit was, got out, and told the admins that they need to fix it. If someone broke into my car without doing any damage to it and then left a note giving me suggestions I'd welcome it, it's not like they drove off with the car and they might have saved my car from future theft.

[Reply to This | Parent]

- Re:Great Excuse by sms (Score.1) Saturday September 06, @11:52AM
- Re:Great Excuse by laing (Score:1) Saturday September 06, @11:52AM
  - Re:Great Excuse by alienw (Score:2) Saturday September 06, @03·33PM
    - 1 reply beneath your current threshold.
- Re:Great Excuse by rikkards (Score:3) Saturday September 06, @01:29PM
- Re:Great Excuse by Anonymous Coward (Score:1) Saturday September 06, @01:47PM
- Re: Your fly is open by Ignis Flatus (Score.1) Saturday September 06, @01:56PM
- 2 replies beneath your current threshold.
  o Get permission, get paid. by FreeLinux (Score:2) Saturday September 06, @11·12AM
    - 1 reply beneath your current threshold.

Re:Great Excuse (Score:5, Interesting)
by hattig (47930) on Saturday September 06, @10:53AM (#6887147)
(Last Journal: Tuesday August 26, @08:53AM)

Agreed. If he wanted to perform white hat hacking, he should have approached the companies involved and asked for a job to test their security. Hell, he'd have earned money that way as well.

But he did commit a crime - he broke into and entered their systems without permission. Sure, he did it for a good reason in his own head, and wasn't going to be malicious ... but it isn't as if he was doing the internet equivalent of rescuing the baby in a house fire.

[Reply to This | Parent]

> **Re:Great Excuse** (Score:5, Insightful)
> by nearlygod (641860) on Saturday September 06, @11:01AM (#6887191)
>
> How different is this from the investigative reporters on your local news broadcast. In many cases a white hat my find that customer's CC numbers or SS numbers are accessible via an exploit or weak security. In a way, he/she would be helping the public by giving the company and opportunity to correct the situation or at least take it public. An investigating reporter may find that a company or governemnt office is throwing out sensitive info without shredding it or taking the proper preventative measures. If I am giving a company like Amazon my CC#, I want to oknow that they are going to protect that info. Who is going to watch/audit the company if they get lazy?
>
> [Reply to This | Parent]
>
> > - Re:Great Excuse by jjhlk (Score:1) Saturday September 06, @02.39PM
> > - Re:Great Excuse by mindstrm (Score:1) Saturday September 06, @02·42PM
> > - Re:Great Excuse by mindstrm (Score:1) Saturday September 06, @02:44PM
> > - Re:Great Excuse by bitflip (Score·1) Saturday September 06, @03:00PM
> > - Re:Great Excuse by mariox19 (Score:1) Saturday September 06, @04:23PM
> > ○ 1 reply beneath your current threshold.

- Re:Great Excuse by themassiah (Score·1) Saturday September 06, @10:56AM
  - ○ Re:Great Excuse by moonbender (Score:3) Saturday September 06, @11:32AM
  - ○ 2 replies beneath your current threshold.
- Re:Great Excuse by LostCluster (Score:2) Saturday September 06, @10:57AM
  - ○ Re:Great Excuse by SSJVegeto2001 (Score:1) Saturday September 06, @11:18AM
    - Re:Great Excuse by Shanep (Score:2) Saturday September 06, @12:34PM
  - ○ 1 reply beneath your current threshold.
- Re:Great Excuse by Spicerun (Score:1) Saturday September 06, @10·58AM
- Re:Great Excuse by AArmadillo (Score:1) Saturday September 06, @11:01AM
  - ○ 1 reply beneath your current threshold.

Re:Great Excuse (Score:5, Interesting)
by moonbender (547943) <moonbender AT t-online DOT de> on Saturday September 06, @11:02AM (#6887197)
(http://moonbender.host.sk/)

So if someone had broken into my house without permission, then

told me about it afterwards, am I supposed to feel better about it?

That analogy doesn't have a lot of merit. You're a private person, he didn't break into private computers. If a bank has a door to their vault which they don't know of and which is never locked, then yeah, they should be grateful for being told about it. Obviously, there's no bank so stupid, but that just goes to show that banks have a lot more experience dealing with real-world break-ins - another reason why this guy should be acknowledged for his deeds, he's making people aware of problems which they are *not* experienced in dealing with.

[Reply to This | Parent]

- o Re:Great Excuse by Sycraft-fu (Score:2) Saturday September 06, @12:07PM
  - ▪ Re:Great Excuse by moonbender (Score:2) Saturday September 06, @12:28PM
- o Re:Great Excuse by Asmodean (Score:1) Saturday September 06, @12:36PM
- o Re:Great Excuse by Nept (Score.2) Saturday September 06, @04:26PM
- o 1 reply **beneath your current threshold.**
- • Can't ask or tell ,... Its just not the same thing by SerpentDrago (Score:1) Saturday September 06, @11:03AM

Re:Great Excuse (Score:5, Insightful)
by qtp (461286) on Saturday September 06, @11:07AM (#6887230)
So if someone had broken into my house without permission, then told me about it afterwards, am I supposed to feel better about it?

But if someone noticed that you can see into your bathroom and bedroom from the street, do you get them busted for being a peeping tom?

The guy's not threatening anyone, nor is he stealing or endangering anyone's life. The "Housebreaking" metaphor doesn't realy apply.

OTOH, your mention of the deadbolt and alarm does apply, but only in the sense that if I did buy/install a deadbolt and alarm, I'd be royally pissed if they didn't work.

[Reply to This | Parent]

Re:Great Excuse (Score:4, Insightful)
by maggard (5579) <maggard@mac.com> on Saturday September 06, @11:17AM (#6887280)

But if someone noticed that you can see into your bathroom and bedroom from the street, do you get them busted for being a peeping tom?

But he didn't just "look in", he went and altered files. And the curtians were down, the door closed, he didn't just happen to glance in but **broke in.**

The guy's not threatening anyone, nor is he stealing or endangering anyone's life. The "Housebreaking" metaphor doesn't realy apply.

Breaking & Entering doesn't mean anyone has to be home or their life

directly threatened.

[Reply to This | Parent]

- Re:Great Excuse by qtp (Score 2) Saturday September 06, @11.31AM
    - Re:Great Excuse by Shanep (Score:2) Saturday September 06, @12.49PM
- altered files? by asv108 (Score:2) Saturday September 06, @12:37PM
    - Re:altered files? by maggard (Score:1) Saturday September 06, @01:55PM
        - Re:altered files? by arose (Score:2) Saturday September 06, @04:05PM
        - Re:altered files? by catenos (Score:2) Saturday September 06, @08:54PM
            - Re:altered files? by maggard (Score 2) Sunday September 07, @01:11AM
            - Re:altered files? by catenos (Score 2) Sunday September 07, @07:35AM
    - **1 reply** beneath your current threshold.
  o Re:Great Excuse by Agent Deepshit (Score:1) Saturday September 06, @11:17AM
    - Re:Great Excuse by qtp (Score:3) Saturday September 06, @11:34AM
        - Re:Great Excuse by Agent Deepshit (Score:1) Saturday September 06, @12:20PM
        - Re:Great Excuse by ionpro (Score:2) Saturday September 06, @12:59PM
        - **2 replies** beneath your current threshold.

Re:Great Excuse (Score:4, Insightful)
by dirk (87083) <dirk@one.net> on Saturday September 06, @11:19AM (#6887294)
(http://cafeleprick.no-ip.com/)

Except we was in the systems and could have done anything while in there. Maybe he is a true "white hat" and didn't do anything bad and told them everything. But it is just as likely that he left a trojan or backdoor in the system. They can't tell what he did or didn't do, so they now have to not only secure their systems against whatever hacks he used to get in, but they have to scour everything on the system to make sure he didn't change any data or leave anything behind (and there is no way to tell whether he copied anything from the system).

[Reply to This | Parent]

- Re:Great Excuse by Piquan (Score:2) Saturday September 06, @07:23PM
    - Re:Great Excuse by dirk (Score:2) Saturday September 06, @10:18PM

Re:Great Excuse (Score:5, Funny)
by Have Blue (616) on Saturday September 06, @11:19AM (#6887296)
(http://slashdot.org/)

> But if someone noticed that you can see into your bathroom
> and bedroom from the street, do you get them busted for
> being a peeping tom?

No, but if he calls me up and says "I was watching you through your bedroom window last night" I would.

[Reply to This | Parent]

[reply to This | Parent]

- Mod parent up. by qtp (Score:2) Saturday September 06, @11:55AM
  - Re:Great Excuse by Snowspinner (Score:1) Saturday September 06, @01:59PM
    - 1 reply beneath your current threshold.
  - Break in by AtariAmarok (Score:2) Saturday September 06, @11:26AM
    - Re:Break in by urmensch (Score:1) Saturday September 06, @11:40AM
    - Re:Break in by efflux (Score:2) Saturday September 06, @01:49PM
      - Deseyres Repeating by qtp (Score:2) Saturday September 06, @04:59PM
  - Re:Great Excuse by frankjr (Score:1) Saturday September 06, @11:32AM
    - 1 reply beneath your current threshold.
  - Your counter-analogy sucks too - try mine. by GreenEggsAndHam (Score:1) Saturday September 06, @12:37PM
    - 1 reply beneath your current threshold.
  - Re:Great Excuse by jjhlk (Score·1) Saturday September 06, @02:43PM
- Re:Great Excuse by practicalista (Score:2) Saturday September 06, @11:25AM
- Re:Great Excuse by lactose99 (Score 1) Saturday September 06, @11:44AM
  - Re:Great Excuse by lactose99 (Score:2) Saturday September 06, @12:32PM
  - 1 reply beneath your current threshold.
- You're a goddamn moron. by Anonymous Coward (Score·1) Saturday September 06, @11:48AM
  - Re:You're a goddamn moron. by LearnToSpell (Score:1) Saturday September 06, @12:50PM
  - Re:You're a goddamn moron. by Acts of Attrition (Score:1) Saturday September 06, @03:57PM
    - 1 reply beneath your current threshold.
  - 1 reply beneath your current threshold.
- Re:Great Excuse by mod_parent_down (Score:1) Saturday September 06, @11:50AM

Re:Great Excuse (Score:5, Interesting)
by MrHanky (141717) on Saturday September 06, @12:01PM (#6887533)
(http://www.google.com/)
An interesting analogy.

After drinking heavily in a bar, a friend of mine and I bought some slices of pizza at a shop, and went outside to eat. Since we were too drunk to stand up, we sat down on the steps outside another shop, which was closed for the night. That is, it should have been. My friend was leaning his back on the door, which was open. He fell right in.

Now, the right thing to do, according to you, would be to go away, minding his own business. And what the hell was he doing, trespassing on the steps outside the shop and all. If this was in Texas, he would be rightfully shot. However, my friend, being both an imbecile and a crook with neither morals, nor respect for private property, went inside to look for a telephone and hopefully the phone number to the owner (we were both too tired to do any serious looting). And so the owner was noticed and the door was closed, and my friend got a serious hangover.

The moral of this story is: if you drink, you get a hangover, so alchohol is bad, 'mkay?

[Reply to This | Parent]

- o Re:Great Excuse by Anonymous Coward (Score:1) Saturday September 06, @01:03PM
  - Re:Great Excuse by MrHanky (Score:2) Saturday September 06, @01·35PM
    - Re:Great Excuse by jjhlk (Score:1) Saturday September 06, @02:46PM
    - Also by mindstrm (Score:1) Saturday September 06, @02:47PM
- Hey, you left your keys in the door by cpopin (Score:1) Saturday September 06, @12:06PM
- Re:Great Excuse by jeffasselin (Score:1) Saturday September 06, @12:25PM
- Re:Great Excuse by ScooterBill (Score.1) Saturday September 06, @12:41PM
  - o Re:custom client by jimsxe (Score:1) Saturday September 06, @12:51PM

Re:Great Excuse (Score:5, Insightful)
by morissm (22885) <morissm AT lexum DOT umontreal DOT ca> on Saturday September 06, @12:48PM (#6887775)
(http://www.lexum.umontreal.ca/)

The home invasion analogy is a very bad one. A home is by its very nature badly protected (you don't spend millions securing it, do you?) but it is also a sanctuary, a place where a break-in results in a certain emotional stigma.

A better analogy would be this one: Suppose that somebody is waiting in an airport's lobby. He has not gone through the security checks yet. While waiting, he notices airport personnel going through what seems to be an unlocked employee-only door. A thought flashes in his mind: "This doesn't seem very secure. I thought airports were supposed to be secure." So he goes to the door and lo and behold, it is unlocked! He goes through it and find a bunch or corridors and doors.

Naturally curious and a little adventurous, our guy wonders how far he can go. He goes forward and manages to get to the departure area WITHOUT going through security. He feels a little proud of having easily broken a system on which governements and airlines has spent millions.

Being a good citizen, our guy then goes to the security counter and shows his finding to the cop. But suddenly, the cop puts cuffs on him and charges him with trespassing and attempting to bypass security in an airport. Of course, the proper action would have been for the guy to go to security as soon as the unlocked door was found. Adrian Lamo should have stopped his investigation at the misconfigured proxy.

However, is it reasonable to charge somebody with a federal crime for having gone a little further in testing the security of a system? Whether is was an airport or NYT's intranet.

I don't think so. The FBI can claim that they don't know whether the guy smuggled dope during his attempt and the NYT can claim that they'll have to check every system for backdoors but I believe it's mostly bad faith from people lashing out because they felt humiliated. Get a grip... fix your stuff and move on. Destroying the life of somebody who tried to help you is just stupid and cruel.
[Reply to This Parent]

[unreadable | ...]

- oh good by waspleg (Score:2) Saturday September 06, @01:31PM
  - Re:Great Excuse by Qrlx (Score:1) Saturday September 06, @01:41PM
  - Re:Great Excuse by CaptainTux (Score:1) Saturday September 06, @01:56PM
  - Re:Great Excuse by linkjunkie (Score:1) Saturday September 06, @02:05PM
  - my struggle... by C10H14N2 (Score:1) Saturday September 06, @04:18PM
  - **6 replies beneath your current threshold.**

- stupid lame 'grey hats' by xtturbo (Score:1) Saturday September 06, @10:49AM

  - Re:stupid lame 'grey hats' by krumms (Score:2) Saturday September 06, @12:22PM

- Damn straight he should be arrested by Servo (Score:3) Saturday September 06, @10:50AM

  - He got what he deserved by nuggz (Score:2) Saturday September 06, @10:56AM
    - Mens rea by yerricde (Score:1) Saturday September 06, @11:34AM
  - Re:Damn straight he should be arrested by FunkyELF (Score:1) Saturday September 06, @11:03AM
    - Re:Damn straight he should be arrested by The Unforgiven (Score:1) Saturday September 06, @11:08AM
  - Re:Damn straight he should be arrested by Anonymous Coward (Score:1) Saturday September 06, @11:15AM
    - Re:Damn straight he should be arrested by the_2nd_coming (Score:1) Saturday September 06, @11:56AM
    - Re:Damn straight he should be arrested by the_greywolf (Score:1) Saturday September 06, @02:35PM
    - **1 reply beneath your current threshold.**
  - Re:Damn straight he should be arrested by Epistax (Score:2) Saturday September 06, @11:46AM
  - Re:Damn straight he should be arrested by Idou (Score:2) Saturday September 06, @11:52AM
    - Day of the dumbass by Servo (Score:2) Saturday September 06, @12:27PM
      - Re:Day of the dumbass by Idou (Score:2) Saturday September 06, @03:14PM
        - Re:Day of the dumbass by Servo (Score:2) Saturday September 06, @04:42PM
          - Re:Day of the dumbass by Idou (Score:2) Saturday September 06, @06:33PM
            - Re:Day of the dumbass by Servo (Score:2) Saturday September 06, @07:22PM
            - Re:Day of the dumbass by Idou (Score:2) Saturday September 06, @07:57PM
            - Re:Day of the dumbass by Servo (Score:2) Saturday September 06, @10:17PM
  - Re:Damn straight he should be arrested by Mt. Honkey (Score:2) Saturday September 06, @11:54AM
    - Re:Damn straight he should be arrested by Servo (Score:2) Saturday September 06, @12:20PM
      - Re:Damn straight he should be arrested by Mt._Honkey (Score:1) Monday September 08, @12:40AM
    - Re:Damn straight he should be arrested by dtrent (Score:1) Saturday September 06, @12:52PM
  - Re:Damn straight he should be arrested by Laughable (Score:1) Saturday September 06, @02:18PM

06, @02:18PM

- Damn the law by bshroyer (Score:2) Saturday September 06, @02:25PM

Call to "The Screen Savers" (Score:5, Informative)
by Larkfellow (265776) on Saturday September 06, @10:51AM (#6887134)
(http://comic.skilledinsanity.com/)
Here's a link to The Screen Savers (on Tech TV) that has some information about what
Adrian had to say [techtv.com] when he called in live to speak with Leo.
[Reply to This]

- Re:Call to "The Screen Savers" by FearedThought (Score:1) Saturday September 06,
  @04:40PM
- 1 reply beneath your current threshold.

hacking... (Score:5, Insightful)
by softspokenrevolution (644206) on Saturday September 06, @10:52AM (#6887135)
Well, zero tolerance. The thing here is that to an awful lot of people, and especially
those who make the laws, hacking is hacking is hacking, who cares what someone says
they were doing it for.

I can realy understand how someone could consider that they're doing a service for
admins and all of that, but the point is that you are still breaking into a system and then
turning around and saying, "hey, this is a security hole, you should fix it" is kind of
like G. Guido coming down to your house, breaking in through a window with a golf-
club and then saying, "Hey, I can break into your house, better listen to me or I'll do it
again."

I'm sure that Adrian has some noble goals, but fundamentally when a company decides
that they don't like people creeping into their system and then presses charages against
those who do, it's their right to feel that their security was violated. Good luck to him
really, but there are other ways you can help people protect their network security than
by breaking into them.
[Reply to This]

- Re:hacking... by Felinoid (Score·1) Saturday September 06, @11·03AM
  Re:hacking...a service (Score:4, Interesting)
  by globalar (669767) on Saturday September 06, @11:08AM (#6887233)
  (http://slashdot.com/)
  From the article:
  *"'I hope there will be a time when Adrian can do positive things that everyone
  agrees are positive,'"*

  This service analogy, or the positive light of the grey hacker's actions, does have
  some weight, as the hacker can inform the admins about the specific flaws of
  their system security.

  But then again, any service should be prompted or invited. And a larger problem
  is this isn't just washing windows, these are problem areas, flaws, and security
  flaws at that. These might even give access to a company's dirty laundry. So not

ιιαws αι ιιιαι. ιιισου ιιιιgιιι υνιιι gινυ αυυυsq ιυ α υυιιιμαιιy s ιιιιιy ιαιιιιιy. υυ ιιυι
only is this service uninvited and not approved, it gives access to private
company resources and information, and uses the security holes to get in.

Yes, I assume if security is the only dimension that your job entails, then this is
all worth it. But to most people in charge, and arguably the general populace at
large, this is an intrusion by illegal means.

I personally value my private virtual space. If you get on my computer and get
into my root account, it's an intrusion. Yeah, I will listen to how you did it, but
for your troubles you'll never use my computer again.
[Reply to This | Parent]

- Wish I had mod points for once by jbarket (Score:2) Saturday September 06, @11:10AM
    o Re:Wish I had mod points for once by williewang (Score.1) Saturday September
      06, @11:33AM
    o 1 reply beneath your current threshold.

Re:hacking... (Score:5, Insightful)
by El Cubano (631386) on Saturday September 06, @11:35AM (#6887387)

*I can realy understand how someone could consider that they're doing a service
for admins and all of that, but the point is that you are still breaking into a
system and then turning around and saying, "hey, this is a security hole, you
should fix it" is kind of like G. Guido coming down to your house, breaking in
through a window with a golf-club and then saying, "Hey, I can break into your
house, better listen to me or I'll do it again."*

*I'm sure that Adrian has some noble goals, but fundamentally when a company
decides that they don't like people creeping into their system and then presses
charages against those who do, it's their right to feel that their security was
violated. Good luck to him really, but there are other ways you can help people
protect their network security than by breaking into them.*

I can see your point, but what he was doing was exposing flaws in the security of
"public" places on the net. How is this any different than when the local news
where I live broke into the nearby international airport's restricted area and did a
report from there (this was about a year after 9/11) to show how lax security had
become again.

When the journalists do it, it is a public service. When a private citizen does it, it
is a crime. WTF? Personally, if I am going to be utilizing the services of these
sites, I want to know that they have good security (and not just because they say
so).

There is no way anyone can convince me that what he was doing was wrong. He
was providing a public service, and if the public is too ungrateful to realize that,
then it is really sad.

It's not like he extorted money from the comapnies, or demanded some
compensation, heck he even *helped* them fix the holes. It is just sickening that
you can't even be a good Samaritan without someone wanting to take your head
off.

[Reply to This | Parent]
    o 2 replies beneath your current threshold.
• 5 replies beneath your current threshold.

Go Mom! (Score:5, Insightful)
by The Tyro (247333) on Saturday September 06, @10:53AM (#6887140)
Heheh... when the agents wanted to come into her home, she told them to get stuffed and come back with a warrant...

That's love, folks.

It would be ironic if this was set up by the NYtimes. I thought investigative/secret camera/sting operation reporting was supposed to be agressive journalism... couldn't his "hack" be considered the same sort of thing? "Unsporting" doesn't begin to describe it, particularly if he was up-front and honest about helping them out. If the NYtimes can investigate, blow the whistle on others, and embarass them into action, I'd say the same card can be played against the Times. "Sour Grapes" anyone?

Yes, he was likely technically in the wrong, no doubt about it, particularly if you adhere to the letter of the rule, rather than the spirit of the rule... even so, this seems a bit heavy-handed.
[Reply to This]

    • Re:Go Mom! by LostCluster (Score.3) Saturday September 06, @11.01AM
        o It brings up another issue by The Tyro (Score:3) Saturday September 06, @11:54AM
            ■ Re:It brings up another issue by cthugha (Score:2) Saturday September 06, @10.36PM
                ■ My understanding by The Tyro (Score:2) Sunday September 07, @01:25AM
                    ■ Re:My understanding by cthugha (Score:2) Sunday September 07, @03:59AM
        o 1 reply beneath your current threshold.
    • Re:Go Mom! by SunPin (Score:3) Saturday September 06, @11:19AM
    • Re:Go Mom! by Drogo Knotwise (Score.1) Saturday September 06, @01:11PM
    • 2 replies beneath your current threshold.

• Seems fair by TheFairElf (Score·3) Saturday September 06, @10:55AM

    • Re:Seems fair by practicalista (Score:1) Saturday September 06, @11:05AM

• Damn by Timesprout (Score:1) Saturday September 06, @10:56AM

This seems unfair (Score:5, Insightful)
by practicalista (686436) on Saturday September 06, @10:57AM (#6887166)
I am not sure what he did at the New York Times can even be considered hacking.

So far as I can tell he set his web proxy to the address of the company infranet, surfed around that, downloaded some documents and used the information contained in these

to get some more.

Whilst I don't approve of hacking per-se, I'd have to say that here, this is very little more than exposing a badly designed web site.

Imagine that you go to you Gas company's online web site, look at the URL and see your account number in it. You think to yourself, I wonder what would happen if I changed one of the digits. You do and lo and behold up pops all the information to another customer.

Now you can go for your 15 minutes of fame and ring up SecurityFocus or you can have a quiet word with the Webmaster of the Gas company - either way, you are not a hacker.

[Reply to This]

- **He accessed an internal network** by mindstrm (Score:1) Saturday September 06, @11:04AM

  Re:He accessed an internal network (Score:5, Insightful)
  by practicalista (686436) on Saturday September 06, @11:16AM (#6887277)
  The law make distinctions between trespass, breaking and entry, armed robbery and so on.

  The guy who wanders around your house is a trespasser not an armed robber. It seems here that a better analogy would be :

  A guy walks in to your unlocked house, boasts about it and you insist that he prosecuted for the worst possible crime he *may* have committed, not the crime he did commit (to walk through an unlocked door).

  [Reply to This | Parent]

  - **Re:He accessed an internal network** by catenos (Score:3) Saturday September 06, @08:37PM
    - **Re:He accessed an internal network** by MegaFur (Score:1) Saturday September 06, @11:28PM
    - **1 reply beneath your current threshold.**
  - **Re:He accessed an internal network** by Uerige (Score:1) Saturday September 06, @02:48PM
    - **1 reply beneath your current threshold.**
  - **2 replies beneath your current threshold.**
  - **Re:This seems unfair** by Anonymous Coward (Score:1) Saturday September 06, @11:12AM
  - **Re:This seems unfair** by davesag (Score:2) Saturday September 06, @07:29PM
  - **2 replies beneath your current threshold.**

- It's **about time.** by FreeLinux (Score:2) Saturday September 06, @10:58AM

  - **Re:It's about time.** by krumms (Score:2) Saturday September 06, @12:28PM

- **Sheesh!** by joto (Score:3) Saturday September 06, @10:58AM

- Re:Sheesh! by WindowLicker916 (Score 1) Saturday September 06, @11:51AM
  - Re:Sheesh! by joto (Score:2) Saturday September 06, @12:14PM
- Re:Sheesh! by serviscope_minor (Score:1) Saturday September 06, @12:01PM

How lame... (Score:4, Funny)
by Jon Abbott (723) on Saturday September 06, @10:58AM (#6887174)
(http://www.eng.fsu.edu/~jabbott)

> *...the FBI has filed charges against [Lamo], and currently has his parents'*
> *house staked out.*

Well that's just... lame-o! [ducks for cover]
[Reply to This]

- another scapegoat by segment (Score.2) Saturday September 06, @10:59AM

  - 1 reply **beneath your current threshold.**

- He did nothing wront, because... by Jacer (Score:2) Saturday September 06, @11:00AM

- Common Sense!! by drakman (Score.1) Saturday September 06, @11:02AM

  - Re:Common Sense!! by serviscope_minor (Score:1) Saturday September 06, @12:06PM
  - 1 reply **beneath your current threshold.**

What was he thinking? (Score:5, Insightful)
by tarranp (676762) on Saturday September 06, @11:04AM (#6887208)
If you break into someone's house, telling him after the fact how yo got in does not
automatically pardon you from the crime...

Had Adrian simply notified the New York Times in a timely manner about the open
proxy servers, he would have been fine and probably accomplished his mission.

Instead, he took his time cracking the system, widening the holes so to speak, and then
went to a reporter(!), of all people.

There is nothing inherently wrong with his desire to improve security. There is nothing
wrong with him looking around the public spaces on the internet for chinks. What was
wrong was that he failed to tell the people maintaining the chinks directly about them,
widened them until he got at valuable data, didn't tell the affected people about the
data he had received, but then went to a third party and told them about the wanging
big hole he had made. I'm sure he views himself as a knight in shining armor, but in
this matter he behaved like a publicity-seeking self-promoter.

Yes, shame on the NYT for misconfiguring their systems, but even more shame on
Adrian for doing something so illegal and counterproductive.

It does not matter if a person thinks he's a good guy, he still does not have carte
blanche to do whatever he wishes.

vianviic to ao wnatcvci nc wishes.
[Reply to This]

- Re:What was he thinking? by FussionMan (Score:1) Saturday September 06, @01:43PM
- Re:What was he thinking? by ChannelX (Score:2) Saturday September 06, @11:26AM
  - 1 reply beneath your current threshold.
- 4 replies beneath your current threshold.

- Enter the Matrix by GillBates0 (Score:1) Saturday September 06, @11:04AM

- Code of Ethics by Maradine (Score:1) Saturday September 06, @11:06AM

- finaly a good analogy by claude_juan (Score:2) Saturday September 06, @11:07AM

  - Re:finaly a good analogy by LostCluster (Score:2) Saturday September 06, @12:19PM

- This is actually good news by weileong (Score:1) Saturday September 06, @11:09AM

  - You're right by KalvinB (Score:2) Saturday September 06, @11:59AM
  - 1 reply beneath your current threshold.

- ADRIAN DON'T COME HOME! by Anonymous Coward (Score:1) Saturday September 06, @11:09AM

Um, what?? (Score:5, Interesting)
by GrouchoMarx (153170) on Saturday September 06, @11:12AM (#6887257)
(http://slashdot org/)
OK, white hat cracking someone is still cracking their system, no matter how benevolent the intent. But this part just makes my blood boil:

French did not know what the specific allegations were, because the charging document is sealed.

Especially in light of this part of another article that people need to spend more time reading:

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

Excuse me, what part of cracking the NY Times is a threat to national security? Why are so many court documents sealed these days? There is NO legitimate reason for securing this sort of charge. Even if the prosecutors were to go as far as claiming he were a terrorist, there's still no nuclear weapons secrets (which we all know by now anyway, despite being classified) in the NY Times payroll database.

He should use that in his defense: because the case was sealed, it's unconstitutional and

~~He should use that in his defense, because the case was sealed, it's unconstitutional and~~ therefore he can't be found guilty.

I don't support this sort of vigilante white hat hacking, but I oppose ignoring the constitution even more.
[Reply to This]

- Re:Um, what?? by mellonhead (Score·1) Saturday September 06, @12:06PM
    - 1 reply beneath your current threshold.
- Re:Um, what?? by One Louder (Score.3) Saturday September 06, @12:39PM
    - Re:Um, what?? by aminorex (Score:2) Sunday September 07, @09·56PM
- 1 reply beneath your current threshold.

Mixed feelings on this issue (Score:5, Insightful)
by Orion Blastar (457579) on Saturday September 06, @11:12AM (#6887262)
If he was hired to test security it would be a different matter. But he allegedly broke into those systems without permission. That puts him in violation of Cybercrime laws.

I feel sorry for him, because he did allegedly report the weaknesses to the admins and he could have just read the data and not told anyone and used the information for his on purposes. So his intentions were good, to plug security holes by finding them and telling the admins about it. But he is doing it the wrong way, without permission.

He may want to think about pleading guilty and making a deal to get reduced charges. This will make him famous and when he gets out of jail and ends probation, he can become a security consultant. Otherwise they may try to make an example out of him and charge him with a full pentalty and any other charges they can think of.

But then the places he broke into didn't use good security practices and didn't apply the latest updates. Personally, I wouldn't put a machine on the Internet that contains sensitive data on it that only my company should have access to like contact information, credit card numbers, etc.
[Reply to This]

- Re:Mixed feelings on this issue by Daedalus-Ubergeek (Score:1) Saturday September 06, @11:30AM
    - Re:Mixed feelings on this issue by Orion Blastar (Score:1) Saturday September 06, @05:11PM
    - 1 reply beneath your current threshold.
- Re:Mixed feelings on this issue by ratboy666 (Score:2) Saturday September 06, @01:00PM
    - Cybercrime by Orion Blastar (Score.1) Saturday September 06, @05:15PM
    - 1 reply beneath your current threshold.

- Jayson Blair? Ah. by AtariAmarok (Score:3) Saturday September 06, @11:12AM

    - Now HERE is some honesty! by AtariAmarok (Score:2) Saturday September 06, @12:45PM

- Why they're after him by mabu (Score:2) Saturday September 06, @11:13AM

- More likely... by Brian Stretch (Score:2) Saturday September 06, @11:46AM
- Re:Why they're after him by stevejsmith (Score:2) Saturday September 06, @11:51AM

Why do they do it? (Score:5, Insightful)
by Knunov (158076) <eat@my.ass> on Saturday September 06, @11:14AM
(#6887271)
(http://goatse.cx/)

I know what many of you are thinking. Why not tell these companies BEFORE you break in?

Because IT'S NOT FUN, that's why. Or perhaps more accurately, it's not stimulating.

Hacking these sites takes time, and the payoff is getting inside and saying, "WOO-HOO! I DID IT!" The fact that he does nothing malicious afterwards and even calls and helps the sysadmins unfuck their systems is a testament to his character.

For those who would compare his antics to breaking into your home, but not stealing anything, it's a poor analogy. Why? Because your house is your personal meatspace. And if he went inside, he would see many things personal to you, such as family pictures, your kid's toys, or if he was REALLY unlucky, your fat, naked ass sitting in a Lazy Boy with a bowl of chips balanced on your ponderous belly, flipping through the channels.

"Uhhh... hey dude. Your lock is vulnerable."

See? Just not the same.

Getting past a computer's defenses is not the same as physically entering a home or bank vault, though I would find the latter far less intrusive than home invasion, especially if he never even touched the money.

Now, if he LOOKED at personal/confidential files once inside, that is a different story. But beating a system's defenses, with the only ambition of proving you can do it, then calling the responsible party and helping them fix the security flaw SHOULD NOT be punished.

Misdemeanor, at most.

It doesn't matter what he *could* have done while inside, it matters what he did, or more specifically *did not* do while inside the system.

"That bastard! He saw my FILE NAMING SCHEME!"

Yeah, he should fry for that...

Knunov
[Reply to This]

- Re:Why do they do it? by Sycraft-fu (Score:2) Saturday September 06, @11:59AM
- Re:Why do they do it? by buttahead (Score:2) Saturday September 06, @12:59PM
- Re:Why do they do it? by Caeldan (Score:1) Saturday September 06, @01:28PM
- Re:Why do they do it? by RzUpAnmsCwrds (Score:2) Saturday September 06, @07:40PM
- Re:Why do they do it? by eddie can read (Score:1) Sunday September 07, @04:09AM
- **3 replies beneath your current threshold.**

- No more bullshitting. by Henry Stern (Score:2) Saturday September 06, @11.16AM

  - **1 reply beneath your current threshold.**

Hacker the Gray (Score:5, Funny)
by AppHack (622902) on Saturday September 06, @11:18AM (#6887289)
So he's a gray hat hacker who has fallen into shadow. Will he come back as a white hat hacker, more powerful than before?
[Reply to This]

  - lotr jokes ... by krumms (Score:2) Saturday September 06, @12:32PM

- MS upset at free choice?? by Martigan80 (Score:1) Saturday September 06, @11:19AM

  - Re:MS upset at free choice?? by Hatta (Score:2) Saturday September 06, @12:35PM

- Run. Just get out of here... by Jerk City Troll (Score:1) Saturday September 06, @11:20AM

Dialectic (Score:5, Insightful)
by Henry V .009 (518000) <marstrail AT hotmail DOT com> on Saturday September 06, @11:22AM (#6887313)
(http://thrasymachus.typepad.com/thras/ | Last Journal: Monday August 11, @12:39PM)
Everyone enjoys comparing hacking to breaking into someone's house or trespassing on private property. It is not. You cannot be 'inside' someone else's server. (It is doubly impossible given the girth of most hackers.) The physical definitions fall apart. And the metaphorical analogies do not mesh physical property and Turing machines so well.

We can begin with what we do know for sure about hacking. A hacking incident is when someone sends packets of information (in some form and by some medium) from a computer or computers to someone else's computer or computers. Which packets are illegal and which are not? Any exact definition raises problems. You can say that any packets that change the functioning of the target system in an unintended way is hacking. So the ignorance of the owner becomes the limit of what is or is not hacking. Faking an email address on a badly designed sign up page (or using mailinator) might be hacking under that definition. Other definitions are similarly problematic. Currently our legal system tends to default (once it actually gets to jury trial) to the above definition, but (in effect) adds that the act must be highly technical and use specialized tools. (Other definitions exist, and I am of course willing to bust holes in any particular one you care to suggest--so go ahead and suggest them.)

But there is such a thing as computer hacking. Everyone knows that. Even if we cannot have an exact legal definition, we know that some things are clearly computer hacking. What is the best way of creating law (which is now inexact) to deal with this behavior? I would suggest making the motive of the hacker one of the main considerations of law. It is always hard to for legal systems to judge guilt based on motive--and they should not if they can avoid it--but in this case, they must either judge the motive of the victim or the perpetrator. If the motive is vandalism or theft, then the act should be punished. Adrian Lamo's motive appears to have been an act that should not have been punished--though it is highly important to state that we do not yet know the facts.
[Reply to This]

- My house, my property by KalvinB (Score:2) Saturday September 06, @12:05PM
  - Re:My house, my property by Henry V .009 (Score.3) Saturday September 06, @12:18PM
    - Further evidence of our retarded society by KalvinB (Score:3) Saturday September 06, @04:17PM
      - Re:Further evidence of our retarded society by Henry V .009 (Score:2) Saturday September 06, @04:31PM
        - Even more evidence of our retarded society by KalvinB (Score:2) Saturday September 06, @05.18PM
          - Re:Even more evidence of our retarded society by Henry V .009 (Score:2) Saturday September 06, @05:36PM
          - Re:Even more evidence of our retarded society by GoneGaryT (Score:1) Sunday September 07, @04:31PM
          - Re:Even more evidence of our retarded society by GoneGaryT (Score:1) Sunday September 07, @04:40PM
          - **2 replies beneath your current threshold.**
        - **1 reply beneath your current threshold.**
  - Re:My house, my property by qeveren (Score:1) Saturday September 06, @01:19PM
    - Re:My house, my property by KalvinB (Score.2) Saturday September 06, @04:21PM
      - Re:My house, my property by egc4ever (Score:1) Saturday September 06, @06:11PM
      - **1 reply beneath your current threshold.**
- Re:Dialectic by Chester K (Score:2) Saturday September 06, @01:33PM
  - Re:Dialectic by Henry V .009 (Score:2) Saturday September 06, @01:57PM
- Re:Dialectic by goldfndr (Score:2) Monday September 08, @12:59AM
- Re:Dialectic by Henry V .009 (Score:2) Saturday September 06, @12:01PM
  - Re:Dialectic by Henry V .009 (Score:1) Saturday September 06, @12:33PM
    - Re:Dialectic by Henry V .009 (Score:1) Saturday September 06, @01:45PM
      - Re:Dialectic by Henry V .009 (Score:2) Saturday September 06, @02:05PM
        - Re:Dialectic by Henry V .009 (Score:2) Saturday September 06, @02:34PM
        - **1 reply beneath your current threshold.**
      - **1 reply beneath your current threshold.**
    - **1 reply beneath your current threshold.**
  - **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**

- More alarming is ... by dominic.laporte (Score.1) Saturday September 06, @11:22AM

  - 1 reply beneath your current threshold.

- And after this is over...... by micaiah (Score:1) Saturday September 06, @11:30AM

Adrian we're here to help (Score:4, Funny)
by Kurt Russell (627436) on Saturday September 06, @11:30AM (#6887353)
(Last Journal: Wednesday May 28, @01:51AM)
you [spr.org]
[Reply to This]

  - Re:Adrian we're here to help by Theodore Logan (Score:2) Sunday September 07, @06:18AM
  - 1 reply beneath your current threshold.

- Ethical but illegal by r6144 (Score.2) Saturday September 06, @11:31AM

  - Re:Ethical but illegal by Courageous (Score:1) Saturday September 06, @11:56AM
  - 1 reply beneath your current threshold.

- What a joke by Vellocet (Score:2) Saturday September 06, @11:32AM

  - Re:What a joke by Entrope (Score:3) Saturday September 06, @11:50AM
    - Re:What a joke by Vellocet (Score:1) Saturday September 06, @12·32PM
      - 1 reply beneath your current threshold.

- What country does he think he lives in? by Cyno (Score:3) Saturday September 06, @11:37AM

- You're all just mad... by whoda (Score:2) Saturday September 06, @11·39AM

- Am I supposed to cry now? by davmoo (Score.2) Saturday September 06, @11:44AM

  - Re:Am I supposed to cry now? by LostCluster (Score:2) Saturday September 06, @12:27PM
  - Re:Am I supposed to cry now? by dtfinch (Score.2) Saturday September 06, @10:05PM
  - 1 reply beneath your current threshold.

- What we need is an intermediary by capedgirardeau (Score:2) Saturday September 06, @11:48AM

- I have another analogy.... by PalmAddict (Score:1) Saturday September 06, @12:03PM

  - 1 reply beneath your current threshold.

- Wall Street Journal by srichman (Score:2) Saturday September 06, @12:06PM

Oh, because corporations are always trustworthy (Score:5, Insightful)
by the-banker (169258) on Saturday September 06, @12:06PM (#6887571)
I understand most of the arguments against what Lamo did, but there are a few points I want to get off my chest:

1. To all those saying, 'Its like he broke in your house': No it isn't. The machines were connected to the internet, which is a public medium. A house is a physically closed space where courts have rules one can have an expectation of privacy. Nobody can claim that the internet should provide an expectation of privacy - by its very nature of using shared resources it flies in the face of such an argument.

2. I don't know how it needs to be done, but truthfully do you (the collective Slashdot you) trust companies to secure their networks, perform audits and be upfront and honest about their failures? If I were a NYT partner I would be furious that my information may have been publicly accessible, yet I would never have known about its vulnerability without Lamo. How many companies have been hacked, had credit card or other info stolen, and just not said anything about it? When Acxiom was hacked, personal information on individuals was stolen over 8 months before they "discovered" the hack - and the hack was found by Hamilton County, Ohio Prosecutor's office when investigating another case that had come forward. What are the chances that Acxiom KNEW they had been hacked, compromised personal information, and said nothing? I am guessing with the current climate of corporate ethics, a pretty high chance exists that a lot of information is being disseminated by people who stole it and consumers have no idea because the company in question is sweeping it under the rug.

Hacking into someone else's system is bad. Nobody can disagree there, but the bottom line is a tradeoff of negative impacts - for what Lamo did I see a lot fewer negative consequences than today's corporate irresponsibility with personal information and computer security.

[Reply to This]

- Re:Oh, because corporations are always trustworthy by juuri (Score:2) Saturday September 06, @04:09PM
- Re:Oh, because corporations are always trustworthy by gothicpoet (Score:1) Saturday September 06, @07:50PM
- 3 replies beneath your current threshold.

- Breaking into House/Car Analogy by wiredbuddy (Score:1) Saturday September 06, @12:15PM

- First false stories, then shoot the messenger by cpopin (Score.1) Saturday September 06, @12:18PM

  - 1 reply beneath your current threshold.

- Ingrateful by Bruha (Score:2) Saturday September 06, @12:20PM

- Did the Times admins lie on their resumes? by Lodragandraoidh (Score:2) Saturday

- Did the Times admits no on their resumes? by Podragandraokm (Score:2) Saturday September 06, @12:28PM

- why do I have to put a subject by BRUTICUS (Score:1) Saturday September 06, @12:37PM

- Interview him by BortQ (Score:3) Saturday September 06, @12:46PM

- Stupid NY-Times by caffeineHacker (Score:1) Saturday September 06, @12:51PM

- is there such a thing as cracking... by lobsterGun (Score:2) Saturday September 06, @12:52PM

- that's smart thinking... by buttahead (Score:1) Saturday September 06, @12:52PM

- The Problem is how they're handling this by miraclemax (Score:2) Saturday September 06, @12:55PM

    - 1 reply beneath your current threshold.

- Its a sad world by madstork2000 (Score:3) Saturday September 06, @12:58PM

    - Re:Its a sad world by gvc (Score:2) Saturday September 06, @01:29PM

- Isn't INTENT part of committing a crime? by Quizo69 (Score:2) Saturday September 06, @01:02PM

    - Re:Isn't INTENT part of committing a crime? by gvc (Score:1) Saturday September 06, @01:13PM

- New York Times story by cpopin (Score:1) Saturday September 06, @01:10PM

- So I was walking downtown... by ZackSchil (Score:1) Saturday September 06, @01:20PM

All the news thats is fitted to print (Score:5, Insightful)
by cluge (114877) on Saturday September 06, @01:25PM (#6887988)
(http://www.italian-cars.com)

The NYT is one of the most hypocritical organizations today. They sue to get 9/11 tapes of people dieing - all in the name of "openess" and "public information", yet they have a network connected to the public network - which is open and transparent through their own doing - and thats bad/illegal? PLEASE - The NYT's proxy servers were so misconfigured that it was akin to them posting information in the window of the downtown offices and then getting pissed if people read what they posted.

You can bet your rear quarters that if our hacker had been a reporter on a story for the NYT that they would be vigorously defending his actions. Like most large corporate entities the NYT has no moral basis for anything it does, in the end it's about money, not honesty, truth or enlightenment. It sure as hell isn't about the times mission statement which is "The Company's core purpose is to enhance society by creating, collecting and distributing high-quality news, information and entertainment."

Perhaps our hacker should have "enhanced society" by distributing the information he

Perhaps our hacker should have "enhanced society" by distributing the information he found to the world. It would have been high quality news to see how one of the most influtential papers is really run.
[Reply to This]

- Re:All the news thats is fitted to print by bradleyjg (Score:1) Saturday September 06, @06:40PM

- Non-Issue by Visceral Monkey (Score:1) Saturday September 06, @01·34PM

NYT? (Score:4, Funny)
by wolf- (54587) on Saturday September 06, @01:46PM (#6888105)
(http.//www.lobosoft com/)
They were worried he knew just how much of their news was faked.
[Reply to This]

- 1 reply beneath your current threshold.

- Police vs. judiciary by gvc (Score·1) Saturday September 06, @01:50PM

Entering via an open door... (Score:4, Insightful)
by podperson (592944) on Saturday September 06, @01:54PM (#6888143)
(http.//www zip.com.au/~tonio)
If you leave your front door open and I take a look inside your house, what crime have I committed? At most, I am told, trespass. If you left the keys under the mat and I opened the door, it's breaking and entering.

Similarly, if I take your car with the clearly stated intention to return it when I am done (e.g. if I desperately needed to drive someone to the hospital), I haven't stolen it, I've borrowed it -- with or without your permission.

Theft, burglary, etc. are crimes defined in part by the intention of the alleged perpetrator and the damages suffered by the alleged victim.

OTOH we live in a world where one of the first "terrorist" groups targeted by the government after 9/11 were Environmental Activists who destroy machinery but have been careful never to hurt anyone.

But I'm no lawyer.
[Reply to This]

- Re:Entering via an open door... by tiny69 (Score:2) Saturday September 06, @07:46PM
  - Re:Entering via an open door... by podperson (Score·2) Saturday September 06, @10:18PM
    - Re:Entering via an open door... by tiny69 (Score.2) Saturday September 06, @11:19PM
- 1 reply beneath your current threshold.

- Consider The NY Time's Liability by nutznboltz (Score.2) Saturday September 06,

@02:13PM

- I know Adrian. by musingmelpomene (Score:1) Saturday September 06, @02:17PM

- Government agecy for hacking by jjhlk (Score:1) Saturday September 06, @02:34PM

- Legality. by mindstrm (Score:1) Saturday September 06, @02:39PM

    - Re:Legality. by x Golden Hawk x (Score:1) Saturday September 06, @03:29PM
        o Re:Legality. by mindstrm (Score:1) Saturday September 06, @03:36PM
            ▪ Re:Legality. by x Golden Hawk x (Score:1) Saturday September 06, @03:46PM

- Surprising lack of common sense by StormReaver (Score:2) Saturday September 06, @02:52PM

    - 1 reply beneath your current threshold.

- Apparently the NY Times heeded sec zealots by aricusmaximus (Score:1) Saturday September 06, @02:54PM

- Give the NY Times a piece of your mind by aricusmaximus (Score:1) Saturday September 06, @03.09PM

- Legality? by Tellalian (Score:1) Saturday September 06, @03:17PM

- It's all proceeding according to plan. . . by Fantastic Lad (Score:2) Saturday September 06, @03:20PM

- White hat? by Cyberllama (Score:2) Saturday September 06, @06:45PM

- first.... by PhreakOfTime (Score:2) Saturday September 06, @07:03PM

- see by ShadowRage (Score:1) Saturday September 06, @10.53PM

- Adrian Lamo! by TheLoneWolf (Score:1) Monday September 08, @12.32PM

- Re:you got beat by LostCluster (Score:2) Saturday September 06, @10:53AM

- Re:better avoid mom and dads house by deglr6328 (Score:2) Saturday September 06, @01:30PM

- GODDAMN I'M UGLY AND STUPID by pr0ntab (Score:2) Saturday September 06, @11:35PM

- Re:Imagine two countries: by crucini (Score:2) Sunday September 07, @01:56AM

- 29 replies beneath your current threshold.

(1) | 2

FBI(19 cv 1495) 1924

| | | Search |

Oh, I get it!! "The BEACH goes on", huh, SONNY??

[home | awards contribute story | older articles | OSDN | advertise | self serve ad system | about | terms of service | privacy | faq]

b3 -2
b6 -1
b7C -1
b7E -3

STANDOFF
A SUDDEN DEADLY ENDING

LETTER FROM PARIS | WAR PHOTOS OUTSIDE THE U.S. | THE LAST
CHAPTER FOR THE COMMISSION | THE NIKON D2H

VISUAL COMMUNICATION QUARTERLY

FBI(19-cv-1495)-1927

Letter Of The Law

WHO CAN FORGET THE SCENE IN "NETWORK" where Howard Beale, the aging UBS news anchor, tells his viewers: "I want you to get up right now. Get up. Go to your windows, open your windows, and stick your head out, and yell, 'I'm as mad as hell and I'm not going to take this anymore!'"

We need to follow Howard's lead. We need to say that we are as mad as hell because one of our premier law enforcement agencies, the FBI, is mounting a direct assault on our First Amendment freedoms.

This assault comes from FBI Special Agent Christine Howard. She recently sent letters to several news organizations demanding that journalists keep all information they have on Adrian Lamo, a computer hacker who said that he had gained access to *The New York Times* Intranet in 2002. Lamo, a 22 year-old drifter who is also known as the "Homeless Hacker," claims that he accessed a list of *The New York Times* Op-Ed contributors. The list included the social security numbers and home phone numbers of many prominent individuals, including former president Jimmy Carter, former secretary of state James Baker, Warren Beatty, Robert Redford, and James Carville. Lamo has been charged in federal court with computer fraud and unlawful access.

The FBI letters sent to journalists covering Lamo's story warn that all records regarding conversations with Lamo may soon be subpoenaed. The letters, according to The Reporters Committee for Freedom of the Press, include the statement, "you are requested not to disclose this request, or its contents, to anyone."

Agent Howard's letters do not follow Justice Department guidelines on issuing subpoenas to journalists. These guidelines include the requirement that federal prosecutors must pursue all other sources of information before issuing a subpoena to a reporter. In addition, federal prosecutors must also negotiate with a reporter before issuing a subpoena unless the negotiations would compromise an investigation. We believe that the FBI has grossly overreached its authority by threatening journalists with subpoenas while demanding their silence.

The FBI's actions strike at the heart of the First Amendment. Threats of subpoenas and demands for silence violate the traditions and protections afforded to the gathering and publishing of newsworthy information. The FBI must retract its subpoena threats and must withdraw the demands for silence. Anything less will keep Howard Beale at our window, expressing our anger to all in our audience. ∎

FBI(19-cv-1495)-1928

R|O|O|T|S|E|C|U|R|E|.|N|E|T|

THE SECURITY NEWS SITE FOR SYSTEMS ADMINISTRATORS & *HACKERS*

Random Quote: I do not fear computers I fear the lack of them - Isaac Asimov   17:07:07 GMT 11/09/2003

Rootsecure Homepage

About RootSecure

Daily Newsletter

News Archives

SecNews XML Feeds

SecNews Console

Links:

---News Stories

---Videos

---Security

---Hacking

　-Wireless

---Misq'

Downloads:

---Audio Clips

·- Videos

　-PDF Documents

---Perl Scripts

---Win32 Tools

---Other

Reports

Hacker Gear

Win' Error Pic's

ASCII Generator

DDP Forum

Your IP Address

Comments

Chat Room

Live Chat

Ping Webmaster

RootSecure:

 --Contact

---Search

---Publicity

---Affiliates

---Submit News

　Referer Logs

　Syndication

　(RSS/XML Feed)

---Privacy Policy

Hits· 168,974
(Since 06/09/02)

11/09/03 - In Depth: Adrian Lamo, the charges

Accused New York Times hacker Adrian Lamo is charged with two title 18 violations
of U.S.C (United States Code). Specifically section 1030 (a) (5) (A) (ii)
"intentionally accesses a protected computer without authorization, and as a result
of such conduct, recklessly causes damage" and section 1029 (a) (2) "knowingly and
with intent to defraud traffics in or uses one or more unauthorized access devices
during any one-year period, and by such conduct obtains anything of value
aggregating $1,000 or more during that period".

Count one alleges Adrian Lamo used the New York Times private Intranet without
authorization causing damage in excess of $25,000 (the cost of "confirming,
addressing, and repairing" the vulnerabilities) and altering contributors
information. Count two alleges Lamo created, then used five usernames / passwords
to obtain search services from "LexisNexis" valued at over $300,000.

Bringing the charges is Special Agent Christina A. Howard of FBI Cybercrime Task
Force who states:

*In or about late February 2002, I read an article on website SecurityFocus.com
dated February 26, 2002 and entitled "New York Times Internal Network Hacked". The
Article reported that ADRIAN LAMO, the defendant, had hacked into the New York
Times' private intranet…*

Likely based on reading that article, Special Agent Christina contacted the New
York Times who then initiated an internal investigation. The investigation
revealed Lamo had accessed various information ranging from staff lists to social
security numbers and created a new "super user" account. Next after a two-three
month wait another New York Times representative contacted Agent Howard informing
her about compromised usernames / passwords which had been used to access
LexisNexis search facilities. LexisNexis then provided further details including
the IP addresses used to access the service that were found to belong to various
Kinko's locations (which it has been reported Lamo used to carry out computer
intrusions before) in California and search queries including among others "Adrian
Lamo".

Background:

In relation to the case New York Times supplied copies of:

1   Their administrative database (admin_db) / Op-Ed database (Oped_db) both
    before and after the alleged intrusion.
2. Various log files from a proxy server, and the NYT Intranet.
3. An email automatically generated by the creation of a new "super user"
    account.
4. Usernames / passwords created by the new "super user" account relating to
    "LexisNexis".

Special Agent Christina A. Howard has been with the FBI for six and a half years,
and has an undergraduate degree in computer science. She views hackers in general
as those who "discover and explorer vulnerabilities and computer weaknesses in
computer networks and software" and that carry out their activities using "hacker
tools that can be either custom written software code or, as is more common,
software readily available for download on the internet or for purchase"

Related Links:

Adrian Lamo Speaks With Leo Before Arrest, TechTV
Exclusive Video of Lamo's Surrender, TechTV
Adrian Lamo Deposition, FindLaw.com
Lamo surrenders, is released, Security Focus
Adrian Lamo charged with computer crimes, Security Focus
Lamo's Adventures in WorldCom, Security Focus

PRESS RELEASE

✓ AP
✓ UPI
✓ Reuters
✓ Bloomberg Business News

✓ Daily News
✓ Newsday
✓ NY Post
✓ NY Times
✓ Wall Street Journal
✓ Washington Post
USA Today
Gannett Journal-News

New York 1
WCBS-TV (2)
WNBC-TV (4)
WNYW-TV (Fox 5)
WABC-TV (7)
WWOR-TV (UPN 9)
WPIX-TV (WB 11)

TV 55 Long Island
News 12 Long Island
News 12 Westchester
Regional News Network
Univision 41
Telemundo 47

✓ ABC News
✓ CBS News
✓ NBC News
✓ CNN
✓ Fox News Network

WCBS-AM (880)
WINS-AM (1010)
WNYC (NPR)
Hudson Valley Radio News Group

National Public Radio

I-80-872

United States Attorney
Southern District of New York

U.S. CHARGES HACKER WITH ILLEGALLY ACCESSING NEW YORK TIMES COMPUTER NETWORK

JAMES B. COMEY, United States Attorney for the Southern District of New York, and PASQUALE D'AMURO, the Assistant Director in Charge of the New York Office of the Federal Bureau of Investigation, announced that ADRIAN LAMO was charged in Manhattan federal court with hacking into the internal computer network of the New York Times. LAMO surrendered today to federal authorities in Sacramento, California.

According to a two-count criminal Complaint unsealed today in Manhattan federal court, on February 26, 2002, LAMO hacked into the New York Times' internal computer network and accessed a database containing personal information (including home telephone numbers and Social Security numbers)

1

FBI(19-cv-1495)-2014

for over 3,000 contributors to the New York Times' Op-Ed page.

As described in the Complaint, soon after being notified of the computer intrusion, the New York Times conducted an internal investigation and confirmed that an intruder had in fact hacked into its network and accessed the personal information for contributors to the Op-Ed page. In addition, according to the Complaint, the Times determined that the intruder had added an entry to that database for "Adrian Lamo," listing personal information including LAMO's cellular telephone number (415) 505-HACK, and a description of his areas of expertise as "computer hacking, national security, communications intelligence."

The Complaint states that the New York Times later learned that while inside its internal network, LAMO had set up five fictitious user identification names and passwords ("userids/passwords") under the New York Times' account with LexisNexis, an online subscription service that provides legal, news and other information for a fee. The Complaint charges that over a three month period, those five fictitious userids/passwords conducted more than 3,000 searches on LexisNexis; in the month of February 2002, the five userids/passwords conducted approximately 18% of all searches

2

performed under the New York Times account.

According to the Complaint, the unauthorized LexisNexis searches included searches for "Adrian Lamo"; searches for other individuals with the last name "Lamo"; searches using the Northern California home address of LAMO's parents; searches for various reputed hackers; and searches for various known associates of LAMO. The LexisNexis charges incurred by these five accounts was approximately $300,000, according to the Complaint.

In an interview with a reporter from an online publication called "SecurityFocus.Com" later on February 26, 2002, LAMO admitted that he was responsible for the New York Times intrusion, it was charged.

The Complaint also identifies a series of other computer intrusions for which LAMO has acknowledged responsibility in interviews with members of the press. In some instances, according to the Complaint, LAMO personally admitted responsibility for the computer intrusion to representatives of the victimized company, explaining how he hacked their computer network, and providing corroboration that he was, in fact, the intruder. The other intrusions, and the approximate dates according to the charges, are: (1)

Excite@Home, May 2001; (2) Yahoo!, September 2001; (3) Microsoft, October 2001; (4) MCI WorldCom, November 2001; (5) SBC Ameritech, December 2001; and (6) Cingular, May 2003.

LAMO, 22, is scheduled to be presented before a United States Magistrate Judge in Sacramento, California, federal court later today.

If convicted, LAMO faces a maximum sentence of 15 years in prison and a $500,000 fine.

Mr. COMEY praised the investigative efforts of the Federal Bureau of Investigation's Cybercrime Task Force and Computer Hacking and Intellectual Property Squad, and also thanked the New York Times, LexisNexis, Yahoo!, Microsoft, MCI WorldCom, SBC Ameritech, and Cingular for their assistance.

Assistant United States Attorney MARK F. MENDELSOHN is in charge of the prosecution.

The charges contained in the Complaint are merely accusations and the defendant is presumed innocent unless and until proven guilty.

03-216   ###

4

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 2
Page 14 ~ b6 - -5,6; b7C - -5,6;
Page 19 ~ Duplicate;

FD-340a (Rev 11-12-89)

C1   E

(Title)   b3 -2
(File No.)   b7E -3

Item	Date Filed	To be returned Yes No		Disposition
	1/5/02	✓	Orig notes	
	1/5/02	✓	(1) log file of lexis-Nexus for intrusion of Adrian Lamo	
	1/5/02	✓		information
			Security - Lexis-Nexus	
	1/5/02	✓	Original notes (1)	Notes
			(2) Employee Roster	
	2/13/02	✓	Original notes Multiple Kinko's in SF	
	2/13/02	✓	(1) log files / Investigation of lexis-Nexus	
		Regarding Adrian Lamo (CD)		

b3 -2
b6 -2,5,6
b7C -2,5,6
b7E -3

Item	Date Filed	To be returned Yes No		Disposition
(1)	5/8/03	✓	(1) CD-Rom w/ screen captures of Worldcom's intranet done by Adrian Lamo	
(1)	5/8/03	✓	Orig notes (1) Conference call w/ Worldcom	
(1)	5/8/03	✓	(1) CD Rom w/ Files that World com w- hack by Adrian Lamo	
(1)	5/15/02	✓	Interview notes	
(1)	5/20/03	✓	(1) CD ROM containing copy ... lexis Nexus	
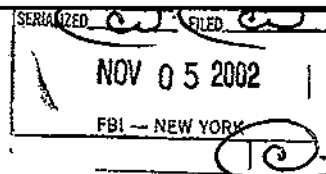
b3 -2
b7E -3

FD-340 (7-19-00)

Universal Case File Number

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document

Date Received _9/19/02_

From

(Name of Contributor)

Kinko's

(Address of Contributor)

b3 -2
b6 -1,6
b7C -1,6
b7E -3

and State)

By

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No
Federal Taxpayer Information (FTI)
☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

b6 -5
b7C -5

SYTEX

9/19/02

**Keep Up With
the Whirlwind**

Kinlo's

SYTEX

Keep Up With
the Whirlwind

- Aug. 25th work away
- comple

PLEASE DO NOT REMOVE
THIS SLIP FROM EXHIBIT

b3 -2
b7E -3

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _NYD_____

Serial # of Originating Document _____

b3 -2
b6 -6
b7C -6
b7E -3

Date Received _07/25/02_____

From _____

Lexis- Nexus

(Name of Contributor)

_____
(Address of Contributor)

_____
(City and State)

By _____

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No

Federal Taxpayer Information (FTI)
☐ Yes ☒ No

Title:

Reference _____
(Communication Enclosing Material)

_____

Description: ☑ Original notes re interview of _____

b6 -6
b7C -6

Information Security- Lexis-nexus

① WHAT IP's WAS HE HITTING? Getting info for me.

② HOW DOES THE REQUEST FOR INFO WORK?

⑩ stole

$300,000⁺ worth of service from servers

NY Times on subscription type of agreement, they were charged for extra activity.

⇒went into lexis.com to access access

[ ] (redacted box)

[ ] (redacted box)

Lexis Nexus.

[ ] (redacted box)

Lexis - Nexus Group

per conversation

b3 -1,2
b6 -5
b7C -5
b7E -3

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ WFO _____

Serial # of Originating Document _____

Date Received _____ 09/20/2002 _____

From _____

(Name of Contributor)

b3 -2
b6 -1,6
b7C -1,6
b7E -3

_____ 325 7th ST. N.W. _____

(Address of Contributor)

_____ Washington DC _____

(City and State)

By _____ SA _____

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference: _____ FD-302 _____

(Communication Enclosing Material)

_____

Description: ☒ Original notes re interview of

① _____ NOTES

② Employee Roster

b6 -6
b7C -6

FBI(19-cv-1495)-2026

3 or 4 months ago. at Kinko's. between 2:3
came in to fax. assisted with fax
engaged in conversation.

outgoing & incoming _____ got impatient.
asked _____ _____ If another
fax had use evening
Thank him. fax trying to resolve
a situation, where computer was
confiscated. Said at library
sitting next to friend surfing
Child porn on his computer,
did not say who took it.

5'11 green eyes (remembered) 165 thin.
No facial hair well groomed. brown.
hair short. T-shirt Jeans..

M-F 9 to 5 over 4 year. now..
No logos..

PLEASE DO NOT REMOVE
~~THIS SLIP FROM EXHIBIT~~

b3 -2
b7E -3

FD-340 (Rev. 3-8-01)

Universal Case File Number

Field Office Acquiring Evidence NYD

Serial # of Originating Document

Date Received 07/10/02

From

(Name of Contributor)

Lexis- Nexus

(Address of Contributor)

(State)

By

To Be Returned ☐ Yes ☐ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No
Federal Taxpayer Information (FTI)
☐ Yes ☐ No

Title:

Reference

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

① log files of Lexis-Nexus
For intrusion - of: Adrian Lamo

PLEASE DO NOT REMOVE
THIS SLIP FROM EXHIBIT

b3 -2
b7E -3

Lexis-nexis files
Adrian Lamo Intrusion

2/10/02

maxell

FD-340 (Rev. 3-8-01)
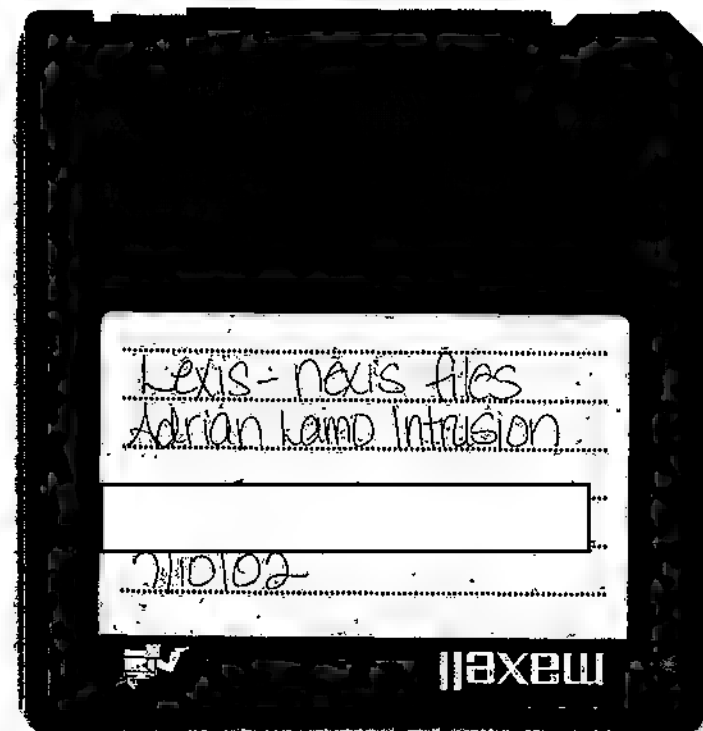
Universal Case File Number _____

Field Office Acquiring Evidence   SAN FRANCISCO , CA

Serial # of Originating Document _____

b3 -2
b6 -1
b7C -1
b7E -3

Date Received _____ 10/16/02 _____

From _____
(Name of Contributor)

_____
(Address of Contributor)

_____
(City and State)

By _____ SA _____

To Be Returned ☐ Yes   ☒ No
Receipt Given ☐ Yes   ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes   ☒ No
Federal Taxpayer Information (FTI)
☐ Yes   ☒ No

Title· ADRIAN LAMO;
New York Times - Victim;
Computer Intrusion;
OO: NY

Reference _____
(Communication Enclosing Material)

b3 -2
b7E -3

Description: ☒ Original notes re interview of

_____ MULTIPLE   KINKOS   IN   SF _____

_____

_____

_____

FBI(19-cv-1495)-2032

Please Do Not Remove

10/16/02

· CHECKED DMV AND FOUND
INFO . . .

ARRON

6 NO SIGN IN PROCEDURE
o CAN USE CREDIT CRD.
o OR KEY CARD YOU
   CAN PUT MONEY
   ON.

TECH 1800 - KINKOS - 4
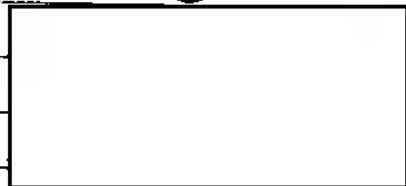
SD FREMONT

↳ EMPLOYEE
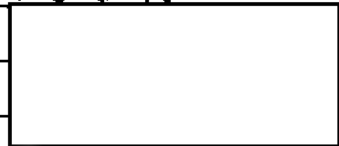
RECOGNIZES HIM

W/in 2-3 weeks

maybe SAT 2:30 - 10:30 pm.

NOT VERY OFTEN.

SO FREMONT.

CP 10.20.18.122

63.164.145.161

NOT GOING ANYWHERE   SAC

"CONTROL" ILLEGITAMATE

BUT NO RESOURCES

SM

1597 Slout KINKO'S

10/22/02

135 ^{00} + SHIPPING

Looks Familiar

$3P-11P$

FD-340 (7-19-00)

Universal Case File Number

Field Office Acquiring Evidence N40

Serial # of Originating Document

Date Received 11/12/2002

From Lexis-Nexus

(Name of Contributor)

(Address of Contributor)

(City and State)

By

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☐ No
Federal Taxpayer Information (FTI)
☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

① LOG-FILES / INVESTIGATION. OF LEXIS- NEXUS
REGARDING ADRIAN -- LAMO (CD)

FD-340 (Rev. 3-8-01)

Universal Case File Number

Field Office Acquiring Evidence **NYO**

Serial # of Originating Document

Date Received **03/21/02**

From **WORLDCOM**

(Name of Contributor)

(Address of Contributor)

(City and State)

By

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☐ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

① CD-Rom containing screen captures of Worldcom's Intranet done by Adrian Lamo.

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence __**NYU**_____ b3 -2
                                                          b7E -3

Serial # of Originating Document _____

Date Received ____**6/7/02**____

From _**Conference call w/ WorldCom**_____
                    (Name of Contributor)

_____
                    (Address of Contributor)

_____
                    (City and State)

By _____

To Be Returned   ☐ Yes   ☒ No
Receipt Given   ☐ Yes   ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)
                  ☐ Yes   ☒ No

Title:

Reference: _____
                    (Communication Enclosing Material)

Description: ☒ Original notes re interview of
(1) Conference Call w/ WorldCom
                                                          b6 -2
                                                          b7C -2

                                    FBI(19-cv-1495)-2040

anything said or
did was priviledged.

6/7/02

Report

- Call into to public relations
voicemail
spoke w/
PR related informed by (A)
that he gained entrance to
internal network

_____ informed, not
aware, conf. call was

_____ Said Lamo would be able to
talk to them

Called Lamo

Recorded?   Cell phone?

- 10³⁰ AM → Said willing to meet;
Sign non-disclosure,
said wanted nothing in
return, Said appreciate
if not prosecuted, Signed
non-disclosure. (he did reveal
info → breaking

FBI(19 cv 1495) 2041

Do you consider that he
broke non-disclosure?

non- disclosure,

how he had gotten in, different IP's
he hit, in files he sent, that
recognized voice,

— never saw face to face.
— came into through proxy setup

Intro

— left footprint in files

12/1/01 1st call, found hole in October had other things to do did not get back to several weeks later.

— do not have web server logs,

— 2 on Saturday (calls one on Tuesday (discussed w/him that he could not get back)

— was never authorized entry, no employee

— network from intranet, other then anything that was

$500,000 $483,000

— details came out afterward that he broke non-disclosure

when far beyond what he said he
would, said "WorldCom" would
only have been hacked.

b6 -2
b7C -2
b7D -1

no contact directly.

FBI(19-cv-1495)-2044

FD-340 (Rev. 3-8-01)

Universal Case File Number

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document

Date Received _05/07/2003_

From _WORLD COM_

(Name of Contributor)

b3 -2
b6 -1,2
b7C -1,2
b7E -3

(Address of Contributor)

(City and State)

By

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title:

Reference: _____

(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

① CD-Rom containing files obtained from
WorldCom regarding hack of Adrian Lamo.

FBI(19-cv-1495)-2045

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ NYO

Serial # of Originating Document _____

Date Received _____ 8/27/02

From _____

(Name of Contributor)

SBC

(Address of Contributor)

By _____

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference: _____

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

SBC.

① _____

b3 -2
b6 -1,2
b7C -1,2
b7E -3

b6 -2
b7C -2

[REDACTED] -SBC (

8/27/02 -

[REDACTED] article.

Mention of a phone company

[REDACTED] approached by Newsbytes
white hat hacker, customer info.
xposed urls to see customer
information in course of
emails said he knew Yamo
friend had open netscape netscape
ip address + keyword ⇒ url attack
if index feature turned on ⇒ look
like FTP directory feature was
turned on files became

- reg processes for Ameritech ??
a snapshot was taken of config, if
something broke, would reset
dial
cust acct name + password + email

Validate runnability operationally
- went through directory structure
figured out p

→ 3600 customer runnability
2600 passed called customers
individually

→ pulled web-server logs for
machine

→ have logs back in Feb. 2004
logs indicate Device up is
some still resolved to
venkos most of access other
places, some from dial up
connections

→ Aanan Janco claimed vulnerabet
in routers → s dial up

1st exploits from dial up pools
Reflected runnability that way.

came in through customer dial
up accts, have some logs
from dial ups.

→ indirect contact w/ Lamo →
w/ Feb incident decided (not to
talk to him, (not sure if PR
people spoke w/ them,

In 3 weeks later someone who
works in security was approached
by email was (not satisfied w/
what went on wanted to speak
w/ SBC.

- in July contacted person in SBC,
Adrian stated that he did

have something, did not have
anything written up, never heard
another thing from Adrian,

→ Adrian doing on camera interview
w/ NBC, lawyers in NBC shut down

→

→ BC ← new hack

→ Estimate $ will provide.
at a later date.

→ did not provide any screen captures

→

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document _____

Date Received _5/20/03_

From _~~Staff~~ Lexis-Nexus_
(Name of Contributor)

_____
(Address of Contributor)

By _____

To Be Returned ☐ Yes ☐ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☐ No

Federal Taxpayer Information (FTI)
☐ Yes ☑ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

(1) CD-Rom containing tar files
for Lexis Nexus

```
total 5544
drwxr-xr-x    2 24999    214           4096 Apr  9  2002 .
drwxr-xr x    3 root     root          4096 May  6 15:39 ..
-rw-r--r--    1 24999    214          25312 Apr  9  2002 LAMO:APR
 rw-r--r--    1 24999    214        4723983 Mar  8  2002 TIMES:FEB
-rw-r--r -    1 24999    214         429677 Mar 11  2002 TIMES:FEB_MAR
-rw-r--r--    1 24999    214          31943 Mar 13  2002 TIMES:LOCUSTS_FEB
-rw r--r--    1 24999    214           4390 Mar 19  2002 TIMES:LOCUSTS_MAR
-rw-r--r--    1 24999    214         373735 Mar 11  2002 TIMES:MAR
 rw-r--r--    1 24999    214          40185 Mar 28  2002 TIMES:MAR14_27
-rw-r  r--    1 24999    214            284 Apr  8  2002 TIMES:MAR28_APR09
```

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s)   7
Page 25 ~ Duplicate;
Page 31 ~ b6 - -3; b7C   3; b7E - -1;
Page 32 ~ b6 - -3; b7C - -3; b7E - -1;
Page 33 ~ b6 - -3; b7C - -3; b7E - -1;
Page 35 ~ Duplicate;
Page 78 ~ b6 - -3; b7C   3; b7E - -1;
Page 79 ~ b6 - -3; b7C - -3; b7E - -1;

XXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)   X
X   No Duplication Fee X
X   For this Page   X
XXXXXXXXXXXXXXXXXXXXXXXXX

b6 -1,3
b7C -1,3
b3 -2
b7E -3

NOTES O[...]

from
FBI,

9/19

SF

on ACS
not physical
here

(Title)

(File No.)

b3 -2
b7E -3

Item	Date Filed	To be returned Yes / No		Disposition
		JUN 2 ~	X	1) Evidence files from SBC at Lamo's back All
		JUL 3 1 2003	X	
				See
	9/15/03	X	orig Interview notes fo	
	10/8	X	1) CD-Rom w/ Tech T interviews	CD-Rom w/other
			X	Tech T interviews when Lamo was on the run 3) Zip disk w freelamo.com
	10/9	X	interview notes of	see
	"	X	" " w	
	"	X	" " on 9/17/03 - Photo of Adrian
				Lamo shown to Case see
	10/9	X	interview notes of	
				9/18/03 Notes + Photo of Adrian Lamo see
	OCT 1 0 2003	X	1) Arrest paperwork for " " - photos, fingerprints cards, FD-395, arrest log, marshall's form medical form
	OCT 1 0 2003	X	Interview notes	see

b3 -2
b6 -2,3,5
b7C -2,3,5
b7E -3

— See next volume —

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ D40

Serial # of Originating Document ___ 77

b3 -2
b6 -1,2
b7C -1,2
b7E -3

Date Received ___ 6120103

From _____

SBC

(Name of Contributor)

(Address of Contributor)

By _____

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title:

Reference: _____

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

① evidence files from SBc of
Lamo's back

FBI(19-cv-1495)-2055

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ NYO

Serial # of Originating Document _____

b3 -2
b6 -1,3
b7C -1,3
b7E -3

Date Received _____ 9/26/03 _____ 6/27/03

From _____

(Address of Contributor)

By _____ (te)

To Be Returned ☐ Yes ☑ No
Receipt Given ☐ Yes ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
  ☐ Yes ☑ No
Federal Taxpayer Information (FTI)
  ☐ Yes ☐ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interviews of

b6 -2
b7C -2

FBI(19 cv 1495) 2056

- open proxy through IDS [redacted], early November saw evidence implemented safeguards towards end Nov. (over Thanksgiving), got specifics from vendor to turn off, not obvious

- did monitoring to see if activity stopped. Saw proxy outbound from senate.gov (http outbound) Source address was part.

IDS Logs, Keep DB of the events reports that were issued

had packet, some
→ URL requests in packet.

No sniffer.

- IDS reported to be outbound http traffic
↳ ISS
No operational impact.

- more than 1 source IP address.

- did who is but does not remember.

- up for awhile then taken down system problem put back online right before

- proxy was in DMZ. (not inside)

- nothing was changed. do not think have not seen anything, no back doors.

- In 3 weeks time turned on/off.

FD-340b (Rev. 8-7-97)

Universal Case File Number

Field Office Acquiring Evidence ___NYO___

Serial # of Originating Document _____

Date Received ___10/7/03___

From ___Self-generated___
          (Name of Contributor)

_____
                (Address of Contributor)

By [   ]
                (Name of Special Agent)

To Be Returned   ☐ Yes ☒ No

Receipt Given   ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

                ☐ Yes ☒ No

Title:

Reference:_____
                (Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

① CD-Rom containing Tech
TU interviews w/ Lamo

② CD-Rom w/ other Tech TU
interviews when Lamo was
on the run

③ zip disk w/ freelamo.com.

                                    FBI/DOJ

FD-340 (7-19-00)

Universal Case File Number _____

Field Office Acquiring Evidence   _OC_ _____

Serial # of Originating Document _____

                                             b3 -2
                                             b6 -1,6

Date Received _9/8/2003_ _____
                                             b7C -1,6
                                             b7E -3

From _____

                                   (Name of Contributor)

_____

                                  (Address of Contributor)

_____

                                   (City and State)

By _SA_ _____

To Be Returned   ☐ Yes   ☒ No

Receipt Given   ☐   ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)
                ☐ Yes   ☒ No

Title: ADRIAN LAMO:
     New York Times - Victim;
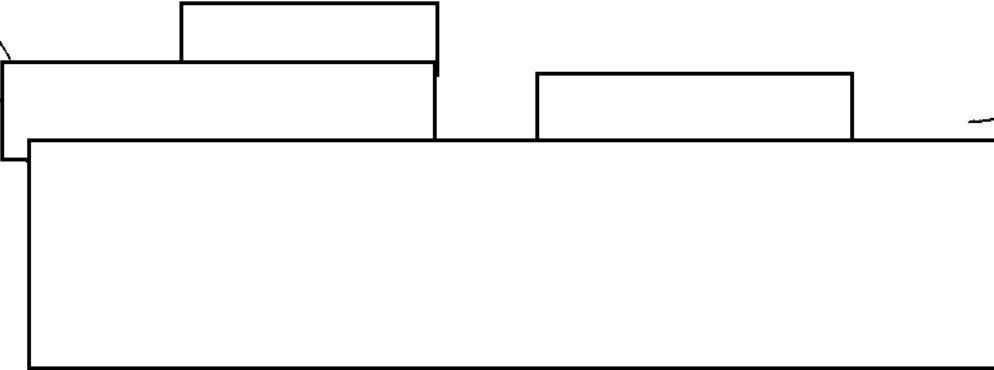   Computer Intrusion;
     OO: NY

Reference: _FD-302_ _____

                      (Communication Enclosing Material)

Description: ☒   Original notes re interview of _____   b6 -6
                                                          b7C -6

9/8/03

①

3/21/76

— web page

Knew him

Talked w/ him   Lasso
still talks w/

[REDACTED]

has a telephone # @ website : adrian . adrian*org

[REDACTED]

Read that A.L. did consulting for WorldCom
Lew Strauss } from newsgroup

- Kinkos is where Lamo reportedly accesses Internet

contact was via aolim not email

[REDACTED]
didn't have a great home life,
was living on own.
smart, brilliant

— Computer [REDACTED]

[REDACTED]

b6 -3
b7C -3

Know [redacted] — [redacted]

[large redacted box]

Adrian may be involved w/ [redacted]

[redacted box]

[redacted] worked @ [redacted]

b6 -5,6
b7C -5,6

[redacted] is in contact w/ [redacted].

[redacted]

if [redacted] was to contact it he could use website see email message thru [redacted]

FD-340 (Rev. 3-8-01)

Universal Case File Number _____ b3 -2-

                                                       b7E -3

Field Office Acquiring Evidence _____

Serial # of Originating Document _____

Date Received _____ 9/15/03 _____

From _____
                                    (Name of Contributor)

_____
                                 (Address of Contributor)

_____
                                  (City and State)

By ___ SA _____

To Be Returned ☐ Yes   ☑ No
Receipt Given   ☐ Yes   ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes   ☑ No
Federal Taxpayer Information (FTI)
                  ☐ Yes   ☑ No

                                                     b6 -1,5
                                                   b7C -1,5

Title: ADRIAN LAMO
        New York Times - Victim
        Computer Intrusion

Reference: _____
                             (Communication Enclosing Material)

Description: ☑ Original notes re interview of

  original notes of the interview w _____

_____

7:30 pm

9/15/03

Conflict user/correct, no schools   basic skills

basic skills

basic skills chat experience , basic skills

b6 -5
b7C -5

LivT -?

1,1 B10

SS#

DOB

work

b6 -5
b7C -5

Questions from List

b7E -1

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ NY _____

Serial # of Originating Document _____

b3 -2
b6 -1
b7C -1
b7E -3

Date Received _____ 09/17/2003 _____

From _____ Self _____

(Name of Contributor)

_____

(Address of Contributor)

_____

By _____ SA _____ FBI NY _____

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title: ADRIAN LAMO;
NEW YORK TIMES - VICTIM;
COMPUTER INTRUSION;
OO: NY

Reference: _____

(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

_____ ON 9/17/2003

b6 -6
b7C -6

— Photo of ADRIAN LAMO Shown to

_____

FBI(19-cv-1495)-2067

9/17/03

(CALL)

b6 -6
b7C -6

WORK

- Adrian Lamo I'D From photo,
  Last contact around

[redacted]

- Member of group [redacted] - publication of

[redacted]

- Relationship [redacted]

[redacted]

⟹ trying to prove a point, Seems to be modest
everyone has a false sense of security, Companies
should be aware of Security Issues.
  Sacrifice Security for Convenience
  accessed to personal ph##, SSN, never offered lists,
  INFORMATION,
  He pointed out problems, But did NOT abuse.
  Showed people & did not exploit his ability.

Lexis/Nexis

[ ]
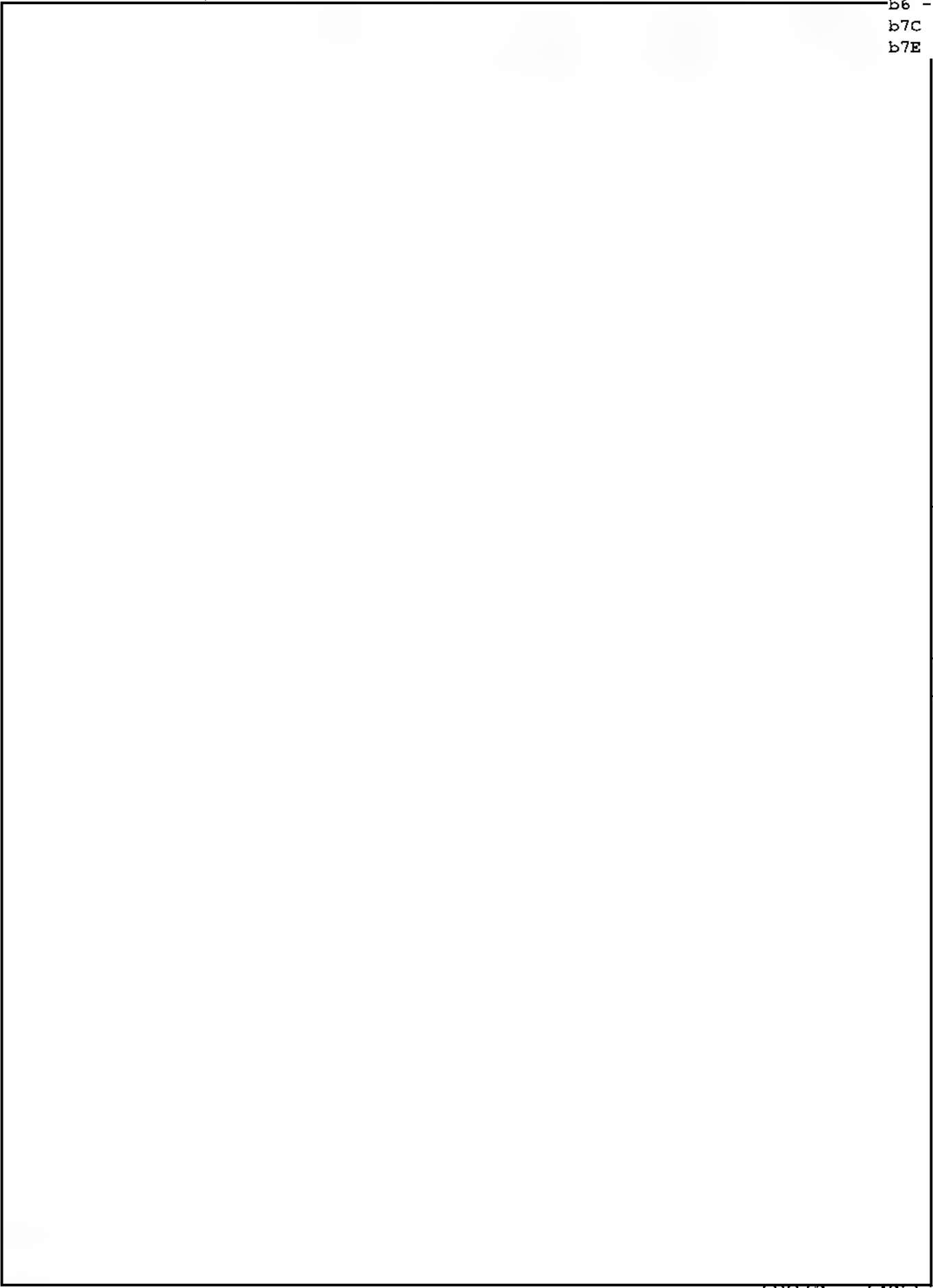
Other

b6 -3,5
b7C -3,5

b) sounds familiar

Screen Name

I)

[ ]

Question Worksheet

Individual background questions

Lamo

might have

info regarding:

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ NY _____

Serial # of Originating Document _____

Date Received ___ 9/18/2003 _____

From ___ Self _____

b3 -2
b6 -1
b7C -1
b7E -3

(Name of Contributor)

_____

(Address of Contributor)

_____

(City and State)

By ___ SA _____

To Be Returned   ☐ Yes   ☑ No
Receipt Given   ☐ Yes   ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
            ☐ Yes   ☑ No
Federal Taxpayer Information (FTI)
            ☐ Yes   ☑ No

Title: ADRIAN LAMO;
NEW YORK TIMES - VICTIM;
Computer INTRUSION;
OO: NY

Reference: _____

(Communication Enclosing Material)

_____

Description: ☑ Original notes re interview of _____

b6 -2
b7C -2

___ 9/18/2003   Notes & Photograph of
ADRIAN LAMO

9/18/2003

[redacted]

Lexis /Nexus

[redacted]

[redacted] Authorized to use Lexus Nexis.

IP Address ~~#~~ / [redacted]

Spam e-mail sent out utilizing
her Name →
ISP AOL [redacted]

[redacted]

[redacted]

use AOL AIM , MSN , Yahoo.

                    reading
2-3 mos. ago "YAHOO headlines about a
"Hacker Challenge" , prize Link to Challenge
no Formal
Computer education. /

Friend [redacted] works For
[redacted]

Friend [redacted] Formerly worked.

⇒ Lexis Nexus password stuck to PC at work
may have been used By other people.

[ ]

Nocharge..com

.MSN

AOL for one year

Yahoo / Instant Messenger

[ ]

[ ] another person at computer

all have own LOGIN Accts.

[ ]

SSN
DO.B
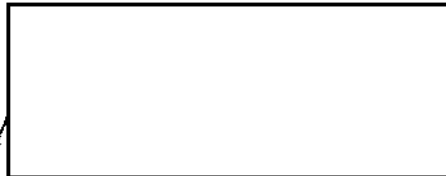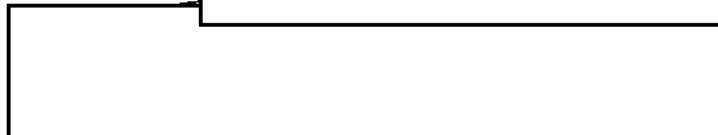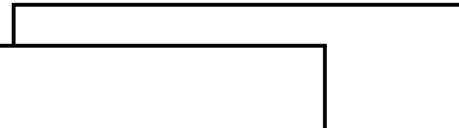
[ ]

[ ]

home ph. #

FD-340b (Rev. 8-7-97)

Universal Case File Number

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document _____

Date Received _09|11|03_

From _ADRIAN LAMO_
<div style="text-align:center">(Name of Contributor)</div>

_____
<div style="text-align:center">(Address of Contributor)</div>

By _____
<div style="text-align:center">(Name of Special Agent)</div>

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

<div style="text-align:center">☐ Yes ☑ No</div>

Title:

Reference:_____
<div style="text-align:center">(Communication Enclosing Material)</div>

_____

Description: ☐ Original notes re interview of

① arrest paperwork for ADRIAN
LAMO - photos, fingerprint cards,
FD-395, ARREST LOG, Marshal's
form, medical forms.

FD-340a (Rev 11-12-89)

(Title) _____

(File No) _____

Item	Date Filed	To be returned			Disposition
		Yes	No		

| LEAVE BLANK | CRIMINAL | | (STAPLE HERE) | | LEAVE BLANK |

STATE USAGE

NFF SECOND

SUBMISSION ☐ APPROXIMATE CLASS ☐ AMPUTATION ☐ SCAR

STATE USAGE

LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX

Lamo,Adrian Alfonso

SIGNATURE OF PERSON FINGERPRINTED

X *G. C. ...* (signature)

SOCIAL SECURITY NO.

042746804

LEAVE BLANK

ALIASES/MAIDEN
LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX

FBI NO.	STATE IDENTIFICATION NO.	DATE OF BIRTH MM DD YY	SEX	RACE	HEIGHT	WEIGHT	EYES	HAIR
		19810220	M	W	N69	130	HAZ	BRO

| 1. R. THUMB | 2. R. INDEX | 3. R. MIDDLE | 4. R. RING | 5. R. LITTLE |

| 6. L. THUMB | 7. L. INDEX | 8. L. MIDDLE | 9. L. RING | 10. L. LITTLE |

Cross Match ID 1000 23184

HP 4100TN

FBI(19 cv 1495) 2083

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY

L. THUMB   R. THUMB

R. CHT FOUR FINGERS TAKEN SIMULTANEOUSLY

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, CLARKSBURG, WV 26306

PRIVACY ACT OF 1974 (P.L. 93-579, REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY NUMBER IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.

JUVENILE FINGERPRINT	DATE OF ARREST	ORI NYFBINY00	
SUBMISSION YES ☐	MM DD YY 20030911	CONTRIBUTOR NYFBINY00 ADDRESS FBI NEW YORK, NY	
TREAT AS ADULT YES ☐	.	REPLY YES ☐ DESIRED?	

SEND COPY TO (ENTER ORI)	DATE OF OFFENSE MM DD YY 20030911	PLACE OF BIRTH (STATE OR COUNTRY) MA	COUNTRY OF CITIZENSHIP US

MISCELLANEOUS NUMBERS	SCARS, MARKS, TATTOOS, AND AMPUTATIONS *NONE*		

	RESIDENCE/COMPLETE ADDRESS 3506 Lynnmar Way, Carmichael, CA, US 95608	CITY	STATE b6 -1 b7C -1

OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER)	LOCAL IDENTIFICATION/REFERENCE	PHOTO AVAILABLE? YES ☒
		PALM PRINTS TAKEN? YES ☐

EMPLOYER: IF U S GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO Unemployed	OCCUPATION *FORMER NETWORK ADMIN*

CHARGE/CITATION	DISPOSITION
1 20030911 2609 - Fraud and Abuse - Computer Hacking	1
2	2.
3	3
ADDITIONAL	ADDITIONAL

ADDITIONAL INFORMATION/BASIS FOR CAUTION	STATE BUREAU STAMP

FBI(19-cv-1495)-2084

FD-249 (REV. 5-11-99)

LEAVE BLANK	CRIMINAL	(STAPLE HERE)		LEAVE BLANK

STATE USAGE

NFF SECOND

SUBMISSION ☐   APPROXIMATE CLASS ☐   AMPUTATION ☐   SCAR ☐

STATE USAGE

WASHINGTON
NEW YORK, NY

LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX

Lamo,Adrian Alfonso

SIGNATURE OF PERSON FINGERPRINTED

X *a.a.*

SOCIAL SECURITY NO

042746804

LEAVE BLANK

ALIASES/MAIDEN
LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX

FBI NO.	STATE IDENTIFICATION NO.	DATE OF BIRTH MM DD YY	SEX	RACE	HEIGHT	WEIGHT	EYES	HAIR
		19810220	M	W	N69	130	HAZ	BRO

1. R. THUMB

3. R. MIDDLE

4. R. RING

5. R. LITTLE

6. L. THUMB

7. L. INDEX

8. L. MIDDLE

9. L. RING

10. L. LITTLE

Cross Match ID 1000 23184

HP 4100TN

FBI(19 cv 1495) 2085

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY

L. THUMB

R. THUMB
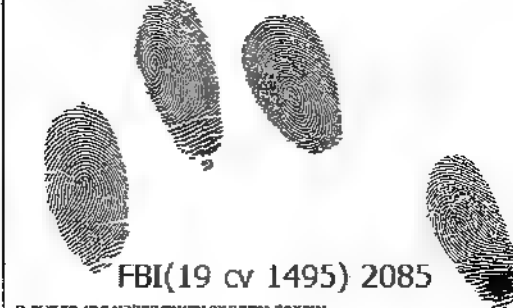
RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

From: Submit

Sent: Thursday, September 11, 2003 2:19 PM

To:

Subject: RE: FBI Submission for lamo

JABS TRANSACTION IDENTIFICATION NUMBER: 577201

EFTS TRANSACTION CONTROL NUMBER: 127.0.0.1.00702
BOOKING NAME: LAMO,ADRIAN ALFONSO
ARREST DATE: 09/11/2003

Fingerprints have been submitted to IAFIS. Response should be sent within 2 hours. This
transaction can be tracked at:

http://149.101.253.5

1

From: Submi[   ]
Sent: Thursday, September 11, 2003 2:45 PM
To:
Subject: RE: JABS Trans Id: #577201--IAFIS RESPONSE RECEIVED

b7E -1,3,9

```
EFTS TRANSACTION CONTROL NUMBER:       127.0.0.1.00702
JABS TRANSACTION IDENTIFICATION NUMBER: 577201
BOOKING NAME:                          LAMO,ADRIAN ALFONSO
ARREST DATE:                           09/11/2003

IAFIS response received: New FBI number assigned.

FBI NUMBER:                            665020CC1
FBI MASTER NAME:                       LAMO,ADRIAN ALFONSO
STATE IDENTIFICATION NUMBER:
```

JABS data is for official criminal justice use only. Unauthorized or improper release is prohibited. Secondary dissemination must be in accordance with NCIC policies and procedures.

IAFIS RAP SHEET ATTACHED

FBI# 665020CC1 SID   OCA

LAMO,ADRIAN ALFONSO   W 509 1981/02/20

FPC   SEX M

HENRY CLASS   API

   NYFBINY00 FBI

          NEW YORK NY   2003/09/11

   A SEARCH OF THE FINGERPRINTS ON THE ABOVE

INDIVIDUAL HAS FAILED TO DISCLOSE PRIOR ARREST

DATA.   CJIS DIVISION

2003/09/11   FEDERAL BUREAU OF INVESTIGATION

NYFBINY00

SPECIAL AGENT IN CHARGE

FEDERAL BUREAU INVEST

23RD FLOOR

26 FEDERAL PLAZA

NEW YORK,NY 10278-0004

ADVICE OF RIGHTS

Place _2u Federal Plaza, NY, NY_
Date _9/11/03_
Time _2:20pm_

YOUR RIGHTS

ALA Before we ask you any questions, you must understand your rights.

_AC A_ You have the right to remain silent.

_4 LA_ Anything you say can be used against you in court.

_A LA_ You have the right to talk to a lawyer for advice before we ask you any questions.

_a/a_ You have the right to have a lawyer with you during questioning.

_c/a_ If you cannot afford a lawyer, one will be appointed for you before any questioning if you wish.

_a/a_ If you decide to answer questions now without a lawyer present, you have the right to stop answering at any time.

WAIVER OF RIGHTS

I have read this statement of my rights and I understand what my rights are. ~~At this time, I am willing to answer questions without a lawyer present.~~

Signed _C. Cote_

b6 -1
b7C -1

Witness

Witness

Time: _2:21pm_

✳ Adrian Lamo does not wish to waive his rights at this time.

FEDERAL BUREAU OF INVESTIGATION
MEDICAL TREATMENT/REFUSAL FORM

DATE: 9/11/03

IF PRISONER REQUIRES OR REFUSES MEDICAL TREATMENT, ARRESTING OFFICIAL WILL COMPLETE THIS FORM PRIOR TO COMMITTING TO ANY CORRECTIONAL FACILITY

NAME: LAST: FIRST: MIDDLE:

DOB 2/20/1981	SSN: 042-74-6804	FBI: INS: OTHER:

b6 -1
b7C -1

CHARGES
NARRATIVE: Computer Intrusion
TITLE: 18   USC: 1030
NARRATIVE:
TITLE: 18   USC: 1029

DATE OF OFFENSE: DATE OF ARREST: 9/11/03

PLACE OF ARREST. New York, NY

ARRESTING OFFICIAL(NAME)	AGENCY/DISTRICT (NYO) FBI - SDNY -	PHONE /24HR

NATURE OF ILLNESS/INJURY: (✓)OLD INJ.   ( )NEW INJ.

tooth infection

IF TREATED BY E.M.S. OR HOSPITAL
FILL OUT THE FOLLOWING

TREATED BY DR./E.M.S.	HOSPITAL: ADMITTED ( )YES (✓)NO
DIAGNOSIS:	MEDICATION PRESCRIBED Over the Counter (✓)YES ( )NO

IF PRISONER REFUSES MEDICAL TREATMENT
FILL OUT THE FOLLOWING

DATE:_____ TIME:_____ PRISONER'S SIGNATURE _____

REMARKS. (PRINT)

has prescription he dropped off today @ Duane Reade

ARRESTEE INFORMATION

Before any arrestee can be processed by the USMS any and all medical problems/conditions must be declared. This form must be completed for each arrestee and given to the responding USMS personnel before the arrestee will be received for processing.

Arrestee name. _Adnan Lamo_

Does arrestee have a prior federal arrest? Circle: (YES) NO

If yes, please list the arrestee's USMS number. _____

If you cannot identify USMS number, please provide arrest information (IE: date, arresting agency, location)
9/9/03, USMS Sacramento

Arrestee's representation for this days proceeding: (Circle) (Legal Aid) CJA retained

If legal aid, has arrestee met with counsel? Circle: (YES) NO

Does the arrestee have any current detainers? Circle: (YES) NO

If yes, please list: _bond $250,000_

Does arrestee have any long term medical condition or conditions (to include: heart problems diabetes, asthma, tuberculosis, HIV, AIDS, hepatitis etc.)? Circle: (YES) NO

Does arrestee require medication/medical attention for this condition? Circle: YES (NO)

Do you, as the arresting agent, currently possess at least one days dosage of the arrestee's medication?
Circle. (YES) NO

Explain: _has heart murmur, taking medication for tooth infection_

Does arrestee have/display/complain of any other medical ailments(IE: broken bones, open wounds etc)? _sometimes_
Circle (YES / NO) @ 234 pm complained of being tired. when gets tired has seizures @ took to hospital.

Does arrestee require medication/medical attention for this condition? Circle: (YES) NO

Do you, as the arresting agent, currently possess at least one days dosage of the arrestee's medication?
Circle YES NO

Explain _____

Is the arrestee a drug addict/user? Circle. YES (NO)

If yes, does this require any special medical program (IE: methadone treatment)? Explain _____

Do you, as the arresting agent, if applicable, possess a medical clearance/fit for confinement letter from a healthcare professional? Circle. (YES) NO (Please attach)

ARRESTEE PROCESSING CHECKLIST

Please check when completed

✓ 1 Have you completed any and all USMS paperwork.
   To include: USMS 312 (Please fill out all forms as completely as possible)

✓ 2 Attached a photo of arrestee to paperwork.

✓ 3 Fingerprint cards
   *1 for USMS file
   *1 for the FBI for FPC classification

✓ 4 Filled out and attached the BOP-9.

✓ 5. Strip searched arrestee

✓ 6. Taken any ~~and all property from the arrestee~~

ARRESTING AGENT: _____   b6 -1
AGENCY: _FBI_   b7C -1
CONTACT # WHILE IN THIS BUILDING: _____

*****NOTE TO ALL ARRESTING AGENTS*****

Be advised, the USMS provides the **COURTESY** of holding and producing arrestee prior to the arrestee's magistrate court appearance. However, the arrestee is not considered a USMS prisoner until a U.S. Magistrate Judge **REMANDS** said arrestee to USMS custody. This means that as the arresting agent, you must be available at all times to respond to any and all matters concerning your arrestee, as you are the responsible party.

United States Marshals Service Policy and Procedures Manual 5.1-1.(a)

Defendant Name	DOB	SSN/	Race	Gender	Arrest Date
Lamo,Adrian Alfonso	02/20/1981	042-74-6804	White	Male	09/11/2003

2

Defendant Name	DOB	SSN	●	Race		Gender ●	Arrest Date
Lamo,Adrian Alfonso	02/20/1981	042-74 6804		Wh te		Male	09.11/2003

Front

Side

1

R-84 (Rev. 5-14-80)

FINAL DISPOSITION REPORT

Leave Blank

Note: This vital report must be prepared on each individual whose arrest fingerprints have been forwarded to the FBI Identification Division without final disposition noted thereon. If no final disposition is available to arresting agency, also obtain subject's right four finger impressions on this form, complete left side and forward the form when case referred to prosecutor and or courts. Agency on notice as to final disposition should complete this form and submit to **Director, FBI, Washington, D.C. 20537, Attention. Identification Division.**
(See instructions on **reverse side**)

FBI No	Final Disposition & Date (if convicted or subject pleaded guilty to lesser charge, include this modification with disposition)
Name on Fingerprint Card Submitted to FBI Last　　　　First　　　　Middle	
Date of Birth_____ Sex_____	
Henry Fingerprint Classification From FBI 1-B Response	
State Bureau No (SID)　　Social Security No (SOC)	This Form Submitted By (Name, Title, Agency, ORI No , City & State)
Contributor of Fingerprints (Include **complete** name and location of agency together with ORI number)	
	Signature　　　　　　Date
	Title
Arrest No (OCA)　　Date Arrested or Received	☐ COURT ORDERED EXPUNGEMENT Return Arrest Fingerprint Card to Contributing Agency, Certified or Authenticated Copy of Court Order Attached
Offenses Charged at Arrest	Right Four Fingers Taken Simultaneously

If additional space is needed, check ☐ and continue on reverse side of this form

FBI(19-cv-1495)-2095

INSTRUCTIONS

1 The purpose of this report is to record the initial data of an individual's arrest and thereafter secure the **final disposition** of the arrest at the earliest possible time from either the arresting agency, the prosecutor or the court having jurisdiction. (INTERIM DISPOSITION INFORMATION, e.g., RELEASED ON BOND, SHOULD NOT BE SUBMITTED) The SUBJECT'S NAME, CONTRIBUTOR AND ARREST NUMBER should be exactly the same as they appear on the fingerprint card IN THE FILES OF THE FBI. The FBI number should be indicated, if known. Agency ultimately making final disposition will complete and mail form to **FBI Identification Division, Washington, D.C. 20537**

2 The arresting agency should list all arrest data on left side of form and obtain the finger impressions of the right four fingers simultaneously. This should be done at the same time as the full set of fingerprints are taken on the arrest fingerprint card. If the arrest is disposed of by the arresting agency, as where the arrestee is released without charge, then the arresting agency should fill in this final disposition and mail form to FBI Identification Division. Of course, if final disposition is known when arrest fingerprint card is submitted it should be noted thereon and this form is then unnecessary. In the event the case goes to the prosecutor, this form should be forwarded to the prosecutor with arrestee's case file

3 **The prosecutor** should complete the form to show final disposition at the prosecution level if the matter is not being referred for court action and thereafter submit form directly to FBI Identification Division. If court action required, the prosecutor should forward form with case file to court having jurisdiction

4 **The court** should complete this form as to final court disposition such as where arrested person is acquitted, case is dismissed, on conviction and when sentence imposed or sentence suspended and person placed on probation

5 When arrested person convicted or enters guilty plea to lesser or different offense than that charged when originally arrested, this information should be clearly indicated

6 If subsequent action taken to seal or expunge record, attach certified or authenticated copy of court order to this form so that FBI can return arrestee's fingerprints to original contributor

7 It is vitally important for completion of subject's record in the FBI Identification Division files that **Final Disposition Report** be submitted in every instance where fingerprints previously forwarded without final disposition noted thereon

---

FOR ADDITIONAL INFORMATION

FBI(19-cv-1495)-2096

FD-597 (Rev 8-11-94)

Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File #

b3 -2
b7E -3

On (date) 9/11/2003

item(s) listed below were:
- ☒ Received From
- ☐ Returned To
- ☐ Released To
- ☐ Seized

(Name) Adrian Lamo

(Street Address) 3506 Lynmar Way,

(City) Carmichael, CA 95608

Description of Item(s):

(1) ORUDIS KT TABLETS
(1) ACID REDUCER
(1) CALIFORNIA IDENTIFICATION CARD D1229973
(1) DUANE READE DRUG CUSTOMER RECEIPT
(1) PAIR Shoelaces
(1) TUMS
(1) Belt black leather
(1) RECEIPT FOR JAMBA JUICE
(1) ONE United Delay Verification receipt
(1) ONE cross pen
(1) one lip balm
(2) succeed slim fast bars
(1) black jacket

Received By

Received From: _____ (Signature)

b6 -1
b7C -1

CALIFORNIA
IDENTIFICATION CARD
D1225

ADRIAN ALFONSO LANO
1755 ALABAMA ST
SAN FRANCISCO CA 94110

SEX: M HAIR: BRN EYES: HZL
HT: 5-09 WT: 130 DOB: 02-20 81

AGE 21 IN 2002

1495)-2098

DR® duane reade drugs

Customer's Receipt

C333462

Waiting

@645
ABS<
CE=MC5400

HUB JAMBA JUICE
SAN FRANCISCO INT'L AIRPORT
SAN FRANCISCO, CALIFORNIA

1161 [   ]

CHK 3960 SEP'0'03 8:49PM GST 1

- - - - - - - - - - - - - - - - - -

1 PEENYA KOWLADA
   VITA BOOST   3.99
      JAMBA BOOST
                           0.69
Subtotal
Tax
Amt Paid   4.68
Cash   0.39
                      5.07
                           5.07
THANK YOU,PLEASE COME AGAIN !!!

UNITED

11SEP03 ORDXS 43190-0   **DELAY VERIFICATION**

AGENT ID: U914

LAMO/ADRIAN

ORIGINALLY HELD SPACE ON:
    UNITED 40 11SEP03 SFO ORD
WAS DELAYED:
    24 HRS.
BECAUSE:
    DELAYED
REACCOMMODATED ON:
    670 ORD TO LGA 11SEP

Res#

L2K950

#ON TIME
Arrivals as shown in
2002 DOT consumer report

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

b3 -2
b6 -5
b7C -5
b7E -3

File # [   ]

On (date) __9/11/03__

item(s) listed below were:
☐ Received From
☒ Returned To
☐ Released To
☐ Seized

(Name [   ]

(Street Address) __52 Duane Street__

(City) __NY, NY__

Description of Item(s): _____

ADRIAN LAMO turned over to the custody
of defense attorney, for night release
to appear tomorrow.

Received By: [   ]   Received From: [   ]

b6 -1,5
b7C -1,5

FBI(19 cv 1495) 2104

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

b3 -2
b7E -3

File # [ ]

On (date) 9/11/03

item(s) listed below were:
☐ Received From
☒ Returned To
☐ Released To
☐ Seized

(Name) ADRIAN LAMO

(Street Address) 3506 LYNNMAR WAY

(City) CARMICHAEL, CA

Description of Item(s):

(1) bLACK beLt
(1) PAIR OF SHOELACES
(1) bottle ACID REDUCER PILLS
(1) bottle OF ORUDIS
(1) identification card CA D1225973
(1) Delay verification UNITED TICKET
(1) Succeed bar
(1) Lip balm
(1) Cross pen
(1) 1/2 Package Tums

FBI(19-cv-1495)-2105

b6 -1
b7C -1

Received By: X _C.C._ (Signature)   Received From: X

NYU Downtown
Beekman 170 William St

Emergency Dept

nurse coordln

(212) 312-5000
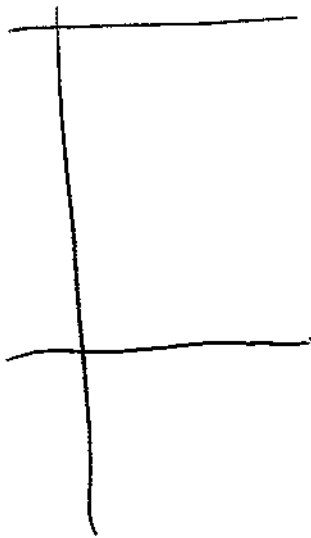
U.S. Department of Justice
United States Marshals Service
USM Form 312. Prisoner Intake

CIRCLE ONE   SAFEKEEPER   (PRISONER LODGED OVERNIGHT IN)   ~~SURRENDER 09/11/2003~~

MCC (NYC) ....MDC(BROOKLYN)..... .. OTHER_____   OR   STREET ARREST

USMS NO	LAST NAME	FIRST NAME	MIDDLE NAME
	Lomo	Adrian	Alfonso

SEX	RACE	HAIR COLOR	EYE COLOR	HEIGHT	WEIGHT
M	W	brown	hazel	5'9"	130

BIRTH DATE	AGE	PLACE OF BIRTH	STATE	CITIZENSHIP
2/20/1981	22	Boston	MASS	

F.B.I. #	SOCIAL SECURITY NO.	I.N.S. ALIEN #
	042-74-6804	

STREET ADDRESS	APARTMENT #	CITY	STATE	ZIP CODE
3506 Lynmmar Way,		Carmichael	CA	95608

TELEPHONE # (AREA CODE)	MARITAL STATUS	EDUCATION LEVEL
(916) 944-1669	Single	GED

BEEPER #	CELL PHONE #
N/A	N/A

ARREST INFORMATION

ARRESTING AGENCY	ADDRESS OF ARREST OR LOCATION	ARREST DATE	AGENCY CASE #
FBI	26 Federal Plaza	9/11/03	

b3 -2
b7E -3

*CHARGE .....MANDATORY.. ....EXAMPLE ... 21 USC 846,....DRUG CONSPIRACY

1030 , 1029

UNIVERSAL PRECAUTIONS.............ΓB, HEPATITUS, ECT... EXPLAIN

_____

DOES ARRESTEE COMPLAIN OF MEDICAL ATTENTION   YES OR (NO) EXPLAIN
tooth infection, over the counter, Duane heade dropped off prescription
heart murmur,

SECURITY CAUTION   YES OR (NO) EXPLAIN

ALIASES, NICKNAMES, STREET NAMES

LAST NAME   FIRST NAME   REMARKS

N/A _____   _____   _____

_____   _____   _____

_____   _____   _____

CO-DEFENDANTS, ASSOCIATES

LAST NAME   FIRST NAME   STREET NAME

N/A _____

STREET ADDRESS   APT. #   CITY   STATE

_____

TELEPHONE # (AREA CODE)   DATE OF BIRTH

_____   _____/_____/_____

REMARKS:_____

CODEFENDENT YES OR NO USMS # _____

_____

LOCALES FREQUENTED, (HANGOUTS)

LOCALE NAME   STREET ADDRESS   APT. #

N/A _____

CITY   STATE   ZIP CODE

_____   _____   _____

TELEPHONE NUMBER   REMARKS

SCARS, MARKS, TATTOOS, PECULIARITIES

N/A _____

_____

VEHICLES

YEAR	MAKE	MODEL	COLOR	PLATE #	STATE	YEAR REGIS
N/A						

REMARKS: _____

LICENSES

LICENSE #.	STATE	TYPE OF LICENSE
Identification Card → #D1225973	CA	

OTHER NUMERICAL IDENTIFIERS

TYPE	NUMBER
PASSPORT	Not current / lost it (expired)
NCIC / NYSID #	
VISA OR GREEN CARD	
OTHER	

EMPLOYMENT

OCCUPATION, TRADE: N/A   FORMER NETWORK ADMIN

EMPLOYER NAME	STREET ADDRESS	CITY	STATE

START DATE   END DATE   POINT OF CONTACT

__/__/__   __/__/__

TELEPHONE # (AREA CODE)   REMARKS

RELATIVES

WIFE, GIRLFRIENDS, CHILDREN, BROTHERS, SISTERS, AUNTS, UNCLES, OTHER RELATIVES RESIDING IN U.S.

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.

ADDRESS : _____ APT. # _____   b6 -5
                                                               b7C -5

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.

ADDRESS : _____ APT. # _____

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.
				/ /

ADDRESS : _____ APT. # _____

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.
				/ /

ADDRESS : _____ APT. # _____

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.
				/ /

ADDRESS : _____ APT # _____

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.
				/ /

ADDRESS _____ APT. # _____

LAST NAME	FIRST NAME	RELATION	PHONE #	D.O.B.
				/ /

ADDRESS : _____ APT. # _____

FINANCIAL INFORMATION

BANK   ACCOUNT TYPE   ACCOUNT NUMBER

N/A

CITY   STATE   BRANCH USED

MILITARY INFORMATION

BRANCH OF SERVICE	MONTH/ YEAR ENTRY	MONTH/ YEAR DISCHARGE	TYPE OF DISCHARGE	RANK AT DISCHARGE
N/A				

REMARKS: _____

PRIOR ARREST RECORD
(LOCAL, STATE & FEDERAL)

AGENCY	DATE OF ARREST	CHARGE
N/A		

REPORTED BY: _____   9/11/03

b6 -1
b7C -1

REVIEWED BY _____

NYU DOWNTOWN HOSPITAL
EMERGENCY DEPARTMENT
AFTERCARE SUGGESTIONS TO PATIENTS

DATE: 9/11/03   TIME: 420 [ ]AM [X]PM

LANO, ADRIAN ZZ
ESCH
7239926   40524 001

NOTE: The examination and treatment you have received in the Emergency Department have been rendered on an emergency basis only and are not intended to substitute for or an effort to provide complete and comprehensive medical care. If you have further questions regarding your emergency care, call the Hospital at (212) 312-5000.

You have been evaluated by the physician and it is felt that you are able to return home. There are, however, things which can make your condition better. These have, or will be discussed with your prior to your departure from the Emergency Department.

DIAGNOSIS: Dental Pain (R/O Dental caries). Medically cleared.

MEDICATIONS RECOMMENDED: Ibuprofen 600 / PCN 500

SPECIAL INSTRUCTIONS: Follow up with Dentist.
Rinse mouth after meals daily
Return to ER if condition worsens

REFERRALS: [X] Your own primary care practitioner or clinic

[ ] Prompt Care Area of the Emergency Department (10A-10P):   [ ] Wound Check

[ ] NYU Downtown Hospital Outpatient Clinics: 170 William Street   Phone: 212-312-5260

Specialty Clinic: _____ Suggested Appointment: _____ days

[ ] NYU Downtown Medical Associates: Dr. _____ Phone: _____

[ ] NYU Downtown Surgery Faculty Practice: Dr. _____ Phone: _____

[ ] Gouvenir Clinics (medicaid applicant referral)   227 Madison Street, NYC   Phone: 212-238-7794

[ ] Downtown Family Care Center   150 Essex Street, NYC   Phone: 212-801-1730

[ ] Brooklyn Primary Care Center   5222 8th Avenue, Brooklyn   Phone: 718-851-8881

[ ] Queens Chinatown Health Clinic   136-26 37th Avenue, Flushing   Phone: 718-886-1200

[ ] Soho OB/GYN Group   135 Spring Street, NYC   Phone: 212-274-0900

[ ] Chinatown Health Clinics   125 Walker Street, NYC   Phone: 212-226-8866

[ ] New York Eye and Ear Hospital   14th Street & 2nd Ave., NYC   Phone: 212-979-4000

[X] NYU Dental Clinics   345 East 24th Street, NYC   Phone: 212-998-9800

[ ] Bellevue Clinics   462 First Avenue, NYC   Phone: 212-562-4721

[ ] Bellevue Psychiatric Center   462 First Avenue, NYC   Phone: 212-562-4230

[ ] Alcohol or Drug Detoxification: Suggest:
   NYUMMTP / Trinity Meth. Program   74 Trinity Place, NYC   Phone: 212-422-0250
   Bellevue Hospital   462 First Avenue, NYC   Phone: 212-562-4141
   Beth Israel (Bernstein Pavillion)   2 Nathan Perlman Place, NYC   Phone: 212-420-2000

[ ] Other Outpatient Department: _____

[ ] Private Practitioner: Specialty: _____

Dr. _____   Phone: _____

FOLLOW-UP IN: 2-3 DAYS

RETURN TO: [ ] WORK [ ] SCHOOL: [X] IMMEDIATELY [ ] IN _____ DAYS _____   DATE

COMMENTS: Medically cleared

INSTRUCTIONS TRANSLATED INTO: _____ by: _____

I hereby acknowledge receipt of and understand the suggestions indicated above. I understand that I have had emergency treatment only, I take the responsibility to arrange for the follow-up care as indicated.

Patient or Guardian _____   9/11/03   Date

W-81 (6/98)

b6 -5
b7C -5

4/03 Date

2:38pm   Nurse a●ved
2:45pm - Stated & made arrangements to go to doctor
           to get medical clearance

2:51pm - allowed to lay down.
2:52pm - 100.1 temperature , blood pressure taken
3:00pm - made arrangements to take to Doctor
3:15pm — transported to hospital,
3:31pm - arrived at hospital
3:33pm - met w/ triage
 3:40pm - met w/ Registration
3:46pm - waiting for Doctor
4:01 - met with Doctor
4:20 - gave 2 ibuprofen
   4:21 - left hospital.
4:32 - arrived Marshal's refused entry
  past 4:30
5:25pm - turned over to the custody of defense attny..

9/12/03

- 10⁰⁵am - received phone call ADRIAN LAMO @ Marshal's
 11³⁰am - went to Marshal's, processed by Marshal's
 11⁵¹am - went to pic-trial, processed by pre-trial
 2⁰⁰pm - walked downstairs get food/drink
 2¹⁵pm - arrived court
 2⁵⁴pm - leaving

ARREST LOG

SUBJECT: Adrian Lamo

ARRESTING AGENTS:

PLACE OF ARREST: 26 Federal Plaza, NY, NY 10278

DATE OF ARREST: 9/11/03

TIME OF ARREST: 1:55pm

TIME ADVISED OF RIGHTS (ORAL & FD-395): 2:20pm

ADVISING AGENT:

TIME SUBJECT SIGNED WAIVER OF RIGHTS:

TIME SUBJECT TRANSPORTED TO FBI OFFICE: N/A

BEGINNING MILEAGE: _____ ENDING MILEAGE: _____

TIME SUBJECT ARRIVED AT FBI OFFICE: N/A

TIME SUBJECT FINGERPRINTED AND PHOTOGRAPHED: 2:02pm

TIME PEDIGREE TAKEN: 1:50pm

TIME INTERVIEW BEGAN: N/A

TIME SIGNED STATEMENT TAKEN: N/A

TIME INTERVIEW CONCLUDED: N/A

TIME SUBJECT TRANSPORTED FOR HEARING/INCARCERATION: 4:24pm from hospital

TIME SUBJECT ARRIVED AT COURT/JAIL: 4:32pm- Marshal's refused because past 4:30pm

PLACE OF INCARCERATION: _____

SUBJECT TURNED OVER TO CUSTODY OF: _____

SUBJECT APPEARED BEFORE US MAGISTRATE: _____

RESULT OF HEARING: _____

RECORD OF REQUESTS: _____

SPECIAL AGENT, FBI   FBI(19 cv 1495) 2115

2:34pm- asked for nurse stated when get tired may have seizures but has not happened in a long time
2:35pm- called Nurse & offered food, coke, anything he needed

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ CV

Serial # of Originating Document _____

Date Received _____ 9-10-03

From _____

_____

_____

By _____ SA _____

b3 -2
b6 -1,5
b7C -1,5
b7E -3

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No

Federal Taxpayer Information (FTI)
☐ Yes ☒ No

Title: ADRIAN LAMO',
New York Times -Victim',
Computer Intrusion',
OO: NY

Reference: _____
(Communication Enclosing Material)

Description: ☒ Original notes re interview of
_____

b6 -5
b7C -5

FBI(19-cv-1495)-2116

9/10/03

Questions for Individuals

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 334
Page 6 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 7 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 8 ~ b6 - -3; b7C - -3; b7E - -1;
Page 9 ~ b6 - -3; b7C - -3; b7E - -1;
Page 11 ~ b6 - -3,5; b7C - -3,5; b7E - -1;
Page 12 ~ b6 - -3; b7C - -3; b7E - -1;
Page 13 ~ b6 - -3; b7C - -3; b7E - -1;
Page 14 ~ b6 - -3; b7C - -3; b7E - -1;
Page 16 ~ b6 - -5; b7C - -5;
Page 24 ~ b6 - -5,6; b7C - -5,6; b7D - -1;
Page 25 ~ b6 - -5,6; b7C - -5,6; b7D - -1;
Page 33 ~ b6 - -2,5; b7C - -2,5;
Page 58 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 59 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 60 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 61 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 64 ~ Duplicate;
Page 65 ~ Duplicate;
Page 66 ~ Duplicate;
Page 67 ~ Duplicate;
Page 68 ~ Duplicate;
Page 69 ~ Duplicate;
Page 70 ~ Duplicate;
Page 71 ~ Duplicate;
Page 72 ~ Duplicate;
Page 73 ~ Duplicate;
Page 74 ~ Duplicate;
Page 75 ~ Duplicate;
Page 76 ~ Duplicate;
Page 77 ~ Duplicate;
Page 78 ~ Duplicate;
Page 79 ~ Duplicate;
Page 80 ~ Duplicate;
Page 81 ~ Duplicate;
Page 82 ~ Duplicate;
Page 83 ~ Duplicate;
Page 84 ~ Duplicate;
Page 85 ~ Duplicate;
Page 86 ~ Duplicate;
Page 87 ~ Duplicate;
Page 88 ~ Duplicate;
Page 89 ~ Duplicate;
Page 90 ~ Duplicate;
Page 91 ~ Duplicate;
Page 92 ~ Duplicate;
Page 93 ~ Duplicate;
Page 94 ~ Duplicate;
Page 95 ~ Duplicate;

```
Page 96 ~ Duplicate;
Page 97 ~ Duplicate;
Page 98 ~ Duplicate;
Page 99 ~ Duplicate;
Page 100 ~ Duplicate;
Page 101 ~ Duplicate;
Page 102 ~ Duplicate;
Page 103 ~ Duplicate;
Page 104 ~ Duplicate;
Page 105 ~ Duplicate;
Page 106 ~ Duplicate;
Page 107 ~ Duplicate;
Page 108 ~ Duplicate;
Page 109 ~ Duplicate;
Page 110 ~ Duplicate;
Page 111 ~ Duplicate;
Page 112 ~ Duplicate;
Page 113 ~ Duplicate;
Page 114 ~ Duplicate;
Page 115 ~ Duplicate;
Page 116 ~ Duplicate;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 119 ~ Duplicate;
Page 120 ~ Duplicate;
Page 121 ~ Duplicate;
Page 122 ~ Duplicate;
Page 123 ~ Duplicate;
Page 124 ~ Duplicate;
Page 125 ~ Duplicate;
Page 126 ~ Duplicate;
Page 127 ~ Duplicate;
Page 128 ~ Duplicate;
Page 129 ~ Duplicate;
Page 130 ~ Duplicate;
Page 131 ~ Duplicate;
Page 132 ~ Duplicate;
Page 133 ~ Duplicate;
Page 134 ~ Duplicate;
Page 135 ~ Duplicate;
Page 136 ~ Duplicate;
Page 137 ~ Duplicate;
Page 138 ~ Duplicate;
Page 139 ~ Duplicate;
Page 140 ~ Duplicate;
Page 141 ~ Duplicate;
Page 142 ~ Duplicate;
Page 143 ~ Duplicate;
Page 144 ~ Duplicate;
Page 145 ~ b6 - -3; b7C - -3;
Page 146 ~ b6 - -3; b7C - -3;
Page 148 ~ b6    5; b7C - -5; b7E - -2;
Page 149 ~ b6 -  5; b7C -  5; b7E -  2;
Page 150 ~ b6 - -5; b7C - -5; b7E - -2;
```

```
Page 151 ~ b7E - -2;
Page 168 ~ b6 - -3; b7C -  3;
Page 169 ~ b6 - -3; b7C - -3;
Page 170 ~ b6 - -3; b7C - -3;
Page 171 ~ b6 - -3; b7C - -3;
Page 172 ~ b6 - -3; b7C - -3;
Page 173 ~ b6 - -3; b7C - -3;
Page 174 ~ b6 - -3; b7C - -3;
Page 175 ~ b6 - -3; b7C - -3;
Page 176 ~ b6 - -3; b7C - -3;
Page 177 ~ b6 - -3; b7C - -3;
Page 178 ~ b6 - -3; b7C - -3;
Page 179 ~ b6 - -3; b7C - -3;
Page 180 ~ b6 - -3; b7C - -3;
Page 181 ~ b6 - -3; b7C - -3;
Page 182 ~ b6 - -3,5; b7C - -3,5;
Page 183 ~ Duplicate;
Page 184 ~ Duplicate;
Page 185 ~ Duplicate;
Page 186 ~ Duplicate;
Page 187 ~ Duplicate;
Page 188 ~ Duplicate;
Page 189 ~ Duplicate;
Page 190 ~ Duplicate;
Page 191 ~ Duplicate;
Page 192 ~ Duplicate;
Page 193 ~ Duplicate;
Page 194 ~ b6 - -3; b7C - -3;
Page 195 ~ b6 - -3; b7C - -3;
Page 196 ~ b6 - -3; b7C - -3;
Page 197 ~ b6 - -3; b7C - -3;
Page 198 ~ b6 - -3; b7C - -3;
Page 199 ~ b6 - -3; b7C - -3;
Page 200 ~ b6 - -3; b7C - -3;
Page 201 ~ b6 - -3; b7C - -3;
Page 203 ~ Duplicate;
Page 205 ~ b6 - -3; b7C - -3; b7E - -2;
Page 206 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 207 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 208 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 209 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 210 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 211 ~ b6 - -3; b7C - -3;
Page 212 ~ b6 - -3; b7C - -3; b7E - -2;
Page 213 ~ b6 - -3; b7C - -3;
Page 214 ~ b6 - -3; b7C - -3;
Page 217 ~ b6 - -3; b7C - -3; b7E - -2;
Page 218 ~ b6 - -3,5; b7C - -3,5; b7E -  2;
Page 219 ~ b6 - -3,5; b7C - -3,5; b7E -  2;
Page 220 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 221 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 222 ~ b6 - -3,5; b7C - -3,5; b7E -  2;
Page 223 ~ b6 -  3,5; b7C - -3,5; b7E -  2;
Page 224 ~ b6 - -3; b7C - -3; b7E - -2;
```

```
Page 225 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 226 ~ b6 - -3,5; b7C -  3,5; b7E -  2;
Page 227 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 228 ~ b6 - -3; b7C - -3; b7E - -2;
Page 229 ~ b6 - -3; b7C - -3; b7E - -2;
Page 230 ~ b6 - -3; b7C - -3; b7E - -2;
Page 231 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 232 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 233 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 234 ~ b6 - -3; b7C - -3; b7E - -2;
Page 235 ~ b6 - -3; b7C - -3; b7E - -2;
Page 236 ~ b6 - -3; b7C - -3; b7E - -2;
Page 237 ~ Duplicate;
Page 238 ~ Duplicate;
Page 239 ~ Duplicate;
Page 240 ~ Duplicate;
Page 241 ~ Duplicate;
Page 242 ~ Duplicate;
Page 243 ~ Duplicate;
Page 244 ~ Duplicate;
Page 245 ~ Duplicate;
Page 246 ~ Duplicate;
Page 247 ~ Duplicate;
Page 248 ~ Duplicate;
Page 249 ~ Duplicate;
Page 250 ~ Duplicate;
Page 251 ~ Duplicate;
Page 252 ~ Duplicate;
Page 253 ~ Duplicate;
Page 254 ~ Duplicate;
Page 255 ~ Duplicate;
Page 256 ~ Duplicate;
Page 257 ~ Duplicate;
Page 258 ~ Duplicate;
Page 259 ~ Duplicate;
Page 260 ~ Duplicate;
Page 261 ~ Duplicate;
Page 262 ~ Duplicate;
Page 263 ~ Duplicate;
Page 264 ~ Duplicate;
Page 265 ~ Duplicate;
Page 266 ~ Duplicate;
Page 267 ~ Duplicate;
Page 268 ~ Duplicate;
Page 269 ~ Duplicate;
Page 270 ~ Duplicate;
Page 271 ~ Duplicate;
Page 272 ~ b6 - -3; b7C - -3;
Page 273 ~ b6 - -3; b7C - -3;
Page 275 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 276 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 277 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 278 ~ b6 -  3; b7C -  3;
Page 279 ~ b6 - -3; b7C - -3;
```

```
Page 280 ~ b6 - -3; b7C - -3;
Page 281 ~ b6 -  3; b7C - -3;
Page 282 ~ b6 - -3; b7C - -3;
Page 283 ~ b6 - -3; b7C - -3;
Page 284 ~ b6 - -3; b7C - -3;
Page 285 ~ b6 - -3; b7C - -3;
Page 286 ~ b6 - -3; b7C - -3;
Page 287 ~ b6 - -3; b7C - -3;
Page 288 ~ b6 - -3; b7C - -3;
Page 289 ~ b6 - -3; b7C - -3;
Page 290 ~ b6    3; b7C    3;
Page 291 ~ b6 - -3; b7C - -3;
Page 292 ~ b6 - -3; b7C - -3;
Page 293 ~ b6 - -3; b7C - -3;
Page 294 ~ b6 - -3; b7C - -3;
Page 295 ~ b6 - -3; b7C - -3;
Page 296 ~ b6 - -3; b7C - -3;
Page 297 ~ b6 - -3; b7C - -3;
Page 298 ~ b6 - -3; b7C - -3;
Page 299 ~ b6 - -3; b7C - -3;
Page 300 ~ b6 - -3; b7C - -3;
Page 301 ~ b6 - -3; b7C - -3;
Page 302 ~ b6 - -3; b7C - -3;
Page 303 ~ b6 - -3; b7C - -3;
Page 304 ~ b6 - -3; b7C - -3;
Page 305 ~ b6 - -3; b7C - -3;
Page 306 ~ b6 - -3; b7C - -3;
Page 308 ~ Duplicate;
Page 310 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 311 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 312 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 313 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 314 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 315 ~ b6 - -3; b7C - -3;
Page 316 ~ b6 - -3; b7C - -3; b7E - -2;
Page 317 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 318 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 319 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 320 ~ b6 - -3; b7C - -3; b7E - -2;
Page 321 ~ b6 - -3; b7C - -3;
Page 322 ~ b6 - -3; b7C - -3; b7E - -2;
Page 323 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 324 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 325 ~ b6 - -3,5; b7C - -3,5; b7E    -2;
Page 326 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 327 ~ b3 - -1; b4 - -1; b6 - -5; b7C - -5; b7D - -1;
Page 328 ~ b3 - -1; b4 - -1; b6 - -5; b7C - -5; b7D - -1;
Page 330 ~ b3 - -1; b4 - -1; b6 -  3; b7C - -3; b7D    1;
Page 331 ~ b3 - -1; b4 - -1; b6 -  3; b7C - -3; b7D    1;
Page 332 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 333 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 334 ~ b3 - -1; b4 - -1; b6 -  3; b7C - -3; b7D    1;
Page 335 ~ b3 - -1; b4 -  1; b6 ~  3; b7C - -3; b7D    1;
Page 336 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
```

```
Page 337 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 338 ~ b3    1; b4 - -1; b6 -  3; b7C -  3; b7D    1;
Page 339 ~ b3    1; b4 - -1; b6 -  3; b7C -  3; b7D    1;
Page 340 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 341 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 342 ~ b3 - -1; b4 - -1; b6 - -3; b7C - -3; b7D - -1;
Page 343 ~ b6    3; b7C - -3;
Page 345 ~ b6    3; b7C - -3; b7E - -2;
Page 346 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 347 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 348 ~ b6    3,5; b7C - -3,5; b7E - -2;
Page 349 ~ b6   -3,5; b7C   -3,5; b7E - -2;
Page 350 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 351 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 352 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 353 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 354 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 355 ~ b6 - -3; b7C - -3;
Page 356 ~ b6 - -3; b7C - -3;
Page 357 ~ b6 - -3; b7C - -3;
Page 358 ~ b6 - -3; b7C - -3;
Page 360 ~ b6 - -3; b7C - -3;
Page 361 ~ b6 - -3; b7C - -3;
Page 362 ~ b6 - -3; b7C - -3;
Page 363 ~ b6 - -3; b7C - -3;
Page 364 ~ b6 - -3,5; b7C - -3,5;
Page 365 ~ b6 - -3,5; b7C - -3,5;
Page 366 ~ b6 - -3; b7C - -3;
Page 367 ~ b6 - -3,5; b7C - -3,5;
Page 368 ~ b6 - -3,5; b7C - -3,5;
Page 369 ~ b6 - -3,5; b7C - -3,5;
Page 370 ~ b6 - -3; b7C - -3;
Page 371 ~ b6 - -3,5; b7C - -3,5;
Page 372 ~ b3 - -1; b6 - -3; b7C - -3;
Page 373 ~ b3 - -1; b6 - -3; b7C - -3;
Page 374 ~ b3 - -1; b6 - -3,5; b7C - -3,5;
Page 375 ~ b3 - -1; b6 - -3,5; b7C - -3,5;
Page 376 ~ b3 - -1; b6 - -3; b7C - -3;
Page 377 ~ b3 - -1; b6 - -3; b7C - -3;
Page 378 ~ b3 - -1; b6 - -3; b7C - -3;
Page 379 ~ b3 - -1; b6 - -3; b7C - -3;
Page 380 ~ b3 - -1; b6 - -3; b7C - -3;
Page 381 ~ b3 · -1; b6 · -3; b7C · -3;
Page 382 ~ b3   -1; b6 · -3,5; b7C   -3,5;
Page 383 ~ b3 - -1; b6 - -3,5; b7C - -3,5;
Page 384 ~ b3 - -1; b6 - -3; b7C - -3;
Page 385 ~ b3 - -1; b6 - -3; b7C - -3;
Page 386 ~ b3    1; b6    3; b7C    3;
Page 387 ~ b3    1; b6    3; b7C    3;
Page 388 ~ b6 - -3; b7C - -3;
Page 394 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
Page 395 ~ b6    3,5; b7C - -3,5; b7E - -2;
Page 396 ~ b6    3,5; b7C -  3,5; b7E - -2;
Page 397 ~ b6 - -3,5; b7C - -3,5; b7E - -2;
```

```
Page 398 ~ b6 - -3; b7C - -3; b7E - -2;
Page 399 ~ b6    3; b7C    3;
Page 400 ~ b6    3; b7C    3;
Page 401 ~ b6 - -3; b7C - -3;
Page 402 ~ b6 - -3; b7C - -3;
Page 403 ~ b6 - -3; b7C - -3;
Page 404 ~ b6    3; b7C    3;
Page 405 ~ b6    3; b7C    3;
Page 406 ~ b6 - -3; b7C - -3;
Page 407 ~ b6 - -3; b7C - -3;
Page 408 ~ b6    3; b7C    3;
Page 409 ~ b6   -3; b7C   -3;
Page 410 ~ b6 - -3; b7C - -3;
Page 411 ~ b6 - -3; b7C - -3;
Page 412 ~ b6 - -3; b7C - -3;
Page 413 ~ b6 - -3; b7C - -3;
```

FD-340a (Rev 11-12-89)

1A Envelope

Case ID: [   ]

)
(File No)

Suppl

Item	Date Filed	To be returned Yes No			Disposition		b3 -2
	OCT 2 1 2003		_Interview notes_		_see serial_		b6 -5,6
	CT 2 1 2003		"	"	"	"	b7C -5,6
	CT 2 1 2003		"	"	"	"	b7E -3
	OCT 2 1 2003		"	"			
			Street Productions		_see serial_		
	OCT 2 3 2003	X	1) _Notes of when tracking down Ramón Elliott into serial_				
	OCT 2 3 2003	X	_Interview_				

1A Envelope

Case ID: [   ]

@	WF 11/17	INTERVIEW NOTES OF [ ]	_recd_ 5 4 20	
@	WF 11/17	INTERVIEW NOTES [ ]	"	
@	NY 11/17	BACKGROUND CKECKS OF: 1		
@	NY 11/17	BACKGROUND CHECKS OF: 11		b3 -2
				b6 -2,3,5,6
				b7C -2,3,5,6
				b7E -3
@	NY 11/17	BACKGROUND CHECKS OF: [ ]		

see next Voluma

FBI(19-cv-1495)-2120

! NY		INTERVIEW NOTES OF	
! NY		INTERVIEW NOTES OF	
! NY		INTERVIEW NOTES OF	
! NY		INTERVIEW NOTES OF 1)	
! NY		1) NOTES OF WHEN TRACKING DOWN LAMOS'S FLIGHT INFO; SEE	
! NY		INTERVIEW NOTES OF	

b3 -2
b6 -5,6
b7C -5,6
b7E -3

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____

Serial # of Originating Document _____

Date Received _____ 9/30/04 _____

From _____
(Name of Contributor)

b3 -2
b6 -1,6
b7C -1,6
b7E -3

_____
(Address of Contributor)

_____
(City and State)

By _SA_ _____

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference: _EC From LV to NY_
(Communication Enclosing Material)

Description: ☒ Original notes re interview of

_____

b6 -6
b7C -6

FBI(19-cv-1495)-2122

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____

Serial # of Originating Document _____

Date Received 9/30/03

From _____

b3 -2
b6 -1,5
b7C -1,5
b7E -3

(Name of Contributor)

_____
(Address of Contributor)

_____
(City and State)

By ___ SA _____

To Be Returned   ☐ Yes   ☒ No
Receipt Given   ☐ Yes   ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
            ☐ Yes   ☐ No

Federal Taxpayer Information (FTI)
            ☐ Yes   ☐ No

Title:

Reference: EC FROM LV TO NY
                    (Communication Enclosing Material)

Description: ☒ Original notes re interview of

b6 -5
b7C -5

FBI(19-cv-1495)-2127

FD-340 (Rev. 8-7-97)

Universal Case File Number _____

Field Office Acquiring Evidence _Boston_

Serial # of Originating Document _____

b3 -2
b6 -1,5
b7C -1,5
b7E -3

Date Received _10/7/03_

From _____
(Name of Contributor)

_____
(Address of Contributor)

By _SA_ _____

To Be Returned ☐ Yes ☐ No
Receipt Given ☐ Yes ☐ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
        ☐ Yes ☐ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interview of _____

b6 -5
b7C -5

Universal Case File Number

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document

Date Received 9|11|03

From

b3 -2
b6 -1,5
b7C -1,5
b7E -3

(Address of Contributor)

By

(Name of Special Agent)

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

☐ Yes ☐ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☑ Original notes re interview of

b6 -5
b7C -5

b6 -5
b7C -5

Adrian Lamo Speaks With Leo Before Arrest

The gray-hat hacker talked with 'The Screen Savers' as he waited to be before turning himself in.

By Tom Merritt

According to SecurityFocus, Adrian Lamo, a famous hacker who exploits security holes and helps companies fix them, is being hunted by the FBI. Lamo called "The Screen Savers" at the top of the show.

Lamo hacked into the website of The New York Times in February 2002 and took the Social Security numbers of several people He then added his name to the list of contributors to The New York Times and notified the paper of what he'd done. The Times responded by threatening to prosecute.

This morning Trigger Street Productions, a multimedia production studio formed by actor Kevin Spacey in 2002, called Leo and mentioned that Lamo's parents were served with a warrant for his arrest The folks at Trigger Street have stayed with Lamo to document his arrest

Adrian Lamo made arrangements with public defenders to turn himself in. He talked to us by phone before he did so.

Two days ago, according to Lamo, the FBI tipped its hand and let him know it wanted him. Lamo said the FBI wanted to search his parents' premises, but his mother refused to let its agents in According to Lamo, the charges might relate to the criminal complaint by The New York Times.

He said he intends to turn himself in after he reviews the charges Although the FBI isn't saying what the charges are, Lamo said he thinks he'll be allowed to know the charges before he turns himself in He expects the charges to be reasonable and he said he'll defend himself rigorously.

"This will not be a slam-dunk prosecution," Lamo said. "[But] I'm worried. I don't know what's going to happen "

Lamo said he didn't know if he would be arrested immediately after he got off the phone.

"It's a shame it had to come to this," he said. "I intend to show that this sort of thing can't be seen as a deterrent. I've done things that people see as illegal and probably are illegal, but I don't think I've done anything wrong."

"I don't think things happen by accident. I don't think that I've done anything wrong. I don't think the FBI is doing anything wrong," he said.

b6 -4,5
b7C -4,5

Lamo said he was going to a safe place to review his legal options after he had talked with us, although his lawyer has advised him to turn himself in as soon as humanly possible. Lamo also said he intends to answer for his actions.

FBI(19 cv 1495) 2135
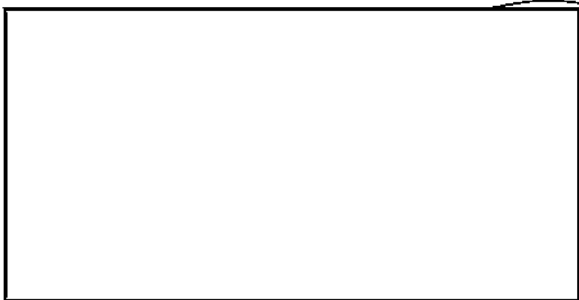
for trigger street

trigger street productions → 7555A North La
Cienega Blvd., Los Angeles, CA

b6 -5
b7C -5

cell
phone. →   called left msg.
            9/9/03

@ triggerstreet.com

Lives in NYC

called to interview, not target (subj):

GJ

Crew head been w/ Lance since late Thursday.

flight info.

Put on notice about preservation letter

$45 pm

$250,000 bond, only $100,000 pre-trial

- ordered to stay with [ ]
  ticket   -9 am Thursday FBI, counselors office

↓ pre-trial

FD-340b (Rev. 8-7-97)

Universal Case File Number [redacted]

Field Office Acquiring Evidence _NYO_

Serial # of Originating Document [redacted]

b3 -2

Date Received _9/11/03_

b6 -1

From _Self generated_

b7C -1

(Name of Contributor)

b7E -3

_____

(Address of Contributor)

By [redacted]

(Name of Special Agent)

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

☐ Yes ☒ No

Title:

Reference:_____

(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

① _notes of when tracking down Lamois flight info_

Sacramento →
to get flight info

627A → United

✷ ✷

Adrian - rescheduled onto Chicago-
LAG
24 SF 10⁰⁰pm, 627ᴬᵐ 10:10am

(LAMO)   flight670
                        spoke w/ United
Wed → 8⁰⁰pm → 8³⁹pm arrived 100 miles →

→ 10¹⁰pm - 6:31 Am whether

→ San Francisco → scheduled

670 → San Francisco

11:2⁰pm other flight

arrived LGA

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ *WFO* _____

Serial # of Originating Document _____

Date Received _____ *9/24/03* _____

From _____

_____

Lavale, MD

(City and State)

By _____ *SA* _____

To Be Returned ☐ Yes ☑ No
Receipt Given ☐ Yes ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☑ No

Federal Taxpayer Information (FTI)
☐ Yes ☑ No

Title: *ADRIAN LAMO;*
New York Times-VICTIM;
COMPUTER INTRUSION;
OO: NY

Reference: _____
(Communication Enclosing Material)

_____

b6 -1,6
b7C -1,6
b3 -2
b7E -3
b7D -1

b6 -5,6
b7C -5,6
b7D -1

Description: ☑ Original notes re interview of

_____

FBI(19-cv-1495)-2140

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _____ WEDINGTON _____

Serial # of Originating Document _____

Date Received _____ 9/25/2003 _____

From _____

(Contributor)

_____
(Address of Contributor)

_____
(City and State)

By _SA_____

b3 -2
b6 -1,2-
b7C -1,2
b7E -3

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No

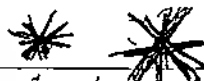Federal Taxpayer Information (FTI)
☐ Yes ☒ No

Title: ADRIAN LAMO,
NEW YORK TIMES-VICTIM;
COMPUTER INTRUSION;
OO:NY

Reference: _____
(Communication Enclosing Material)

_____

Description: ☒ Original notes re interview of

Interview NOTES OF _____

b6 -2
b7C -2

_____

_____

_____

FBI(19-cv-1495)-2143

internal discussions
post intrusion
  Laws contacted someone
  @ WorldCom

Bank of America, Fox news, CitiCorp

~~9/16 Access~~
Reported a call from Washington
post

Checked w/ [ ]
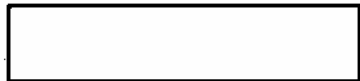
  - telephone
  - e-mail } no
  - met

possible?

= no indention

FBT already in touch w/

Responded to Subpoena
1 yr. ago

Hackers Conference invited by

cy

company had interaction

penetration of the system
###/Dec. 2007
SANS INSTIT. Newsbytes #3, 50
5, 6, 7 Dec. 2007
no malicious, gained
access through proxy
services provided by MCI
$WORLDCOM
web brouse
no 2600 meetings
no contact
not aware of other
intrusions

9/25/2003

DOB:
SSN:

WORK:

dealt w/ side effect
entrusion

Neuer met, don't think
exchanged e-mail

jatt.com.home AT&T Business

AT&T Business
Internet Services

Home | Help Center | > Account Center | About Us

Manage E-mail

Manage User ID

Web Mail
  Check Mail
  New Message
  Address Book
  Distribution Lists
  Spam Control

(LOG OFF)

View Message

From: [   ] SAVE SENDER

To: [   ]

cc :
Date: Thu, September 25, 2003, 10:06:00
Subject: Re: Information Regarding Adrian Lamo
        VIEW HEADER   VIEW BODY

b6 -2,5
b7C -2,5

thanks[   ]

At 01:54 PM 9/25/2003 +0000,[   ]**wrote:**

As discussed[   ]**from my team has been
working with an FBI agent out of New York regarding the
Lamo case. The contact information is as follows:**

Name:[   ]
E-mail
Phone

Please feel free to forward any inquires to myself or
[   ]

Thanks,
[   ]

b6 -1,2,5
b7C -1,2,5

FORWARD MAIL   REPLY   REPLY TO ALL   DELETE   NEXT MESSAGE
RETURN   HELP

Date: Wed, 05 Dec 2001 23:04:17 -0500   b6 -2,5
From: b7C -2,5
Subject:
Sender:
To:
Cc:
X-Mailer: exmh version 2.5 07/13/2001 with nmh-1.0

Hey look, we're famous! Is there any further information on
the nature of the problem?

http://news.excite.com/news/ap/011205/18/worldcom-security

WASHINGTON (AP) - A security hole at telecommunications giant
Worldcom
left internal networks at several of the nation's top companies open
to hackers, according to Worldcom and the security researcher who
discovered the problem.

Adrian Lamo, a consultant in San Francisco, worked with Worldcom to
fix
the months-old problem over the weekend, and the company said there
is
no evidence hackers exploited the security hole.

Internal networks belonging to AOL Time Warner, Bank of America,
CitiCorp, News Corp., JP Morgan, McDonald's Corp., Sun Microsystems
and
many other companies were vulnerable, he said.

"These networks were never designed to be connected to the Internet,"
Lamo said. "They were private circuits running between locations."

The security problem could have allowed hackers to reconfigure or
shut
down the corporate networks, also known as intranets, that are used
for
everything from e-mail to financial transactions.

Worldcom spokeswoman Jennifer Baker said none of Worldcom's customers
were affected.

"Adrian worked very cooperatively with us throughout the weekend,"
Baker
said. "It was a human error on a router."

A router is a device that serves as a traffic light for messages on
computer networks.

b6 -2
b7C -2

Lamo said he found the hole by poking through Worldcom's public Web
site.

"Tons of times there's data that shouldn't be available to anybody
that
is out on a public Web server," Lamo said.

Lamo praised Worldcom's security procedures, and said he used an
unconventional way to enter the company network that is not often
addressed by security experts. He stressed that he didn't attempt to
damage the internal networks.

Within the last several months, Lamo has found security problems at
several major computer firms, including Microsoft and AOL Time
Warner.
In September, he discovered a hole on Yahoo's news site that allowed
him
to alter several stories.

In addition to Worldcom's clients, the company itself was also at
risk,
Lamo said.

Lamo found ways to reset company passwords, give himself all the
computer power of a company director, redirect e-mail and find
personal
information for Worldcom's employees.

"It would have been possible for anyone who was really motivated to
change direct deposit information for employee paychecks to arbitrary
accounts without the employee being notified," Lamo said.

---

b6 -2
b7C -2

Date: Wed, 30 May 2001 09:45:08 -0400
From:
Subject: Internet Policy News
To:
Reply-to
X-Mailer:
Importance: Normal

1. New domains overshadow ICANN meeting in Stockholm
2. ISPs fight spam from the front line
3. Hacker helps Excite@Home toughen defenses
4. Wireless Privacy Legislation Coming

***

May 30, 2001
New domains overshadow ICANN meeting in Stockholm
WASHINGTON (Reuters)

When it meets in Stockholm on Friday, the Internet's top standards-setting
body will still have to fight perceptions that it is too cautious and
bureaucratic -- in essence, that it does not move at ``Internet speed.''

Seven new domains selected by the Internet Corporation for Assigned Names
and Numbers should join the likes of ``.com,'' ''.net'' and ``.org'' by the
end of the year, but hopeful additional applicants are already pushing for a
second round.

``The really serious question now will be how soon we can have new top-level
domains,'' said David Maher, a Chicago attorney who serves as vice president
of public policy for the Internet Society, a group that oversees
infrastructure issues.

In Stockholm, ICANN hopes to set up an oversight panel for the new domains,
get input on how to include regular Internet users in its decisions and take
a firm stance against alternative addressing systems that have sprung up to
provide unofficial domains such as ``.kids'' and ``.xxx.''

ICANN also hopes to get more help around the office with a proposed 20
percent budget increase. The budget could run into resistance from foreign

b6 -5
b7C -5

companies who complain that the organization, which must answer to the U.S. Department of Commerce, has not adequately represented their concerns.

But these issues will take a back seat as anticipation grows over the long-awaited new domains.

`` The real issue now is, `Let's get it going so we can run this grand experiment,''' said Elana Broitman, director of policy and public affairs for Register.com, which is in the process of setting up the .pro domain for doctors, lawyers and other professionals.

CONTROVERSY CONTINUES

Since it was set up by the Clinton Administration in 1998, ICANN has faced pressure to increase the number of available domain suffixes.

ICANN approved seven new domains -- .biz, .info, .pro, .name, .aero, .museum and .coop -- last November, but it rejected 40 others in the process, prompting criticism from commercial interests and Congress that it moved too slowly and selected the domains arbitrarily.

ICANN's decision to allow Mountain View, California-based VeriSign Inc. to retain control of the lucrative .com domain in April also drew charges that it was delaying competition.

ICANN Chairman Vint Cerf told a Congressional panel in February that the group was moving cautiously because it did not know what effect the new domains would have on the world's Internet addressing system.

Commerce Secretary Donald Evans sent a letter to Cerf on Friday encouraging him to pick up the pace.

`` While I recognize ... an attendant need to maintain Internet stability and security, competition and selection are also critical factors. New (domain) entrants represent that promise,'' Evans wrote.

ICANN hopes to translate this desire for greater speed into more manpower. While most registry companies will be happy to pay their share, ICANN could run into resistance from firms that sponsor foreign ``country code'' domains like .uk and .nz that feel they have not been adequately represented in the

past, Maher said.

`` They may be hesitant to contribute to an organization in which they feel they have a relatively minor voice,'' he said.

NO ALTERNATIVES

ICANN will also take a stand against so-called `` alternative root'' systems, which seek to bypass ICANN-mandated standards and set up domains like .tech and .video.

Alternative root companies like New.net Inc. encourage Internet access providers and users to alter their browsers to view their sites. Since most Web users fail to go to the trouble, such domains remain invisible to mainstream audiences.

In a paper posted on the ICANN Web site, President M. Stuart Lynn says the structure of the Internet requires a central authority like ICANN, because alternative roots could direct Web browsers to the wrong sites, or e-mail to the wrong person.

ICANN's deliberate approach to new domains may frustrate some Internet users, Lynn writes, but it is the best way to ensure stability.

`` Impatience in the context of Internet timescales is perfectly understandable. The outcome of orderly processes based on the wishes of the community, however, is assurance that the Internet will continue to function in a stable and holistic manner that benefits the global community, and not become captured by the self-interests of the few,'' he writes.

***

ISPs fight spam from the front line
By Matt Berger
IDG

There is little doubt that you have a grueling job when your business card reads "senior abuse administrator." Scores of computer programmers and techies -- many of whom hold similar job titles -- gathered in San Francisco Thursday at SpamCon 2001 to vouch for the difficulties of their labors.

b6 -5
b7C -5

Technical teams working behind the scenes at ISPs around the world let it be known at the conference that they really despise unsolicited e-mail, commonly known as spam. They gathered there for two days to debate the technical, legal and social effects spam has had on their jobs and the Internet as a whole.

"Spam is definitely a problem for us," said Ava Pettit-Mountain, who works in the abuse department for the Boston-based telecommunication company RCN. "Just in terms of consumer complaints it's definitely got a chilling effect."

Much of Pettit-Mountain's workday is consumed by dealing with customer complaints over the hundreds of thousands of e-mail messages that pass through RCN's network each day. While much of her job is dedicated to tracking down Internet hackers that go about their rogue business on RCN's cable and Internet service, Pettit-Mountain said that more than half of each day is consumed by sorting through complaints and phone calls from customers angry over the junk mail that piles up in their inboxes.

"A lot of customers -- they want a magic button," she said. "We do have some mechanisms in place to block e-mail but obviously we have to be conservative about it."

Abuse departments at ISPs from Earthlink to UUNet Technologies -- each represented at the conference -- offered similar disdain for the overwhelming problem created by mass e-mail marketing, which often is distributed for illegal or unethical purposes. Many of the people attending SpamCon are looking for answers.

"Technologists have always said, 'It's a problem that can be solved with technology.' End users have said, 'Let's sue spammers into oblivion.' I think it's none of the above," said Tom Geller, the director of SpamCon and an author and pundit on the subject.

Finding a solution to spam has, however, left most people stumped. Congress has had little luck on the issue. The House of Representatives Wednesday slimmed down a bill that would protect consumers against unsolicited bulk e-mail.

b6 -5
b7C -5

A representative from the Federal Trade Commission (FTC), one of several
U.S. government organizations belabored with the task of cracking down on
spammers, said Thursday that it has limited resources in aiding consumers in
the fight against bulk e-mail.

"We're not an agency that can set the laws," said Jennifer Mandigo, staff
attorney with the FTC's consumer division. "But the FTC is ready to
generally enforce whatever (Congress) passes."

Ted Gavin, a consultant with Nachman Hays Consulting who is helping to draft
policy against spam for the marketing industry, said that the issue will be
better fought by reaching the people using direct e-mail marketing as an
advertising venue. Many companies selling products or services would have
better luck targeting a specific audience rather than blanketing mailing
lists with spam, Gavin said. Many marketing professionals fall victim to the
fallacy that distributing mass e-mail is low cost.

"The 'Net is not a free resource," Gavin said. "Somebody pays for everything
that gets done on the Internet. There is always a cost associated with
sending an e-mail."

The cost is hard to calculate, Gavin said, but includes the resources ISPs
use to deal with large amounts of data being sent over their networks. The
cost is also borne by consumers who have to pay for the time it takes to
download spam through their ISP. In fact, the European Commission said in a
report earlier this year that spam costs European Internet users about 10
billion euros ($8.57 billion) every year in money spent on Internet
connectivity.

Since the early 1990s, when America Online first took its service to
consumers, the Internet has become a gold mine for direct marketers,
according to Geller. (AOL Time Warner is the parent company of CNN.com.)
Since then, marketing scams such as Ponzi and pyramid schemes have migrated
from mail and newspaper advertisements to the less costly medium. And there
may be no way to get rid of spam if governments, marketers and consumers
don't come to a consensus on a solution.

"I remember e-mail before there was ever marketing, when it was just a bunch
of techies chatting online," Geller said.

Unfortunately, he noted, those days are history.

***

Hacker helps Excite@Home toughen defenses
By Robert Lemos
Special to CNET News.com
May 29, 2001, 5:55 p.m. PT

Not all hackers are bad--just ask Excite@Home.

The company shored up its online defenses after a hacker pointed out a
vulnerability in April that allowed access to the company's internal network
and exposed nearly 3 million support records to the public.

The company praised the hacker--known by the alias "Adrien Lamo"--for coming
forward after he poked around their network.

Lamo contacted the company nearly two months ago after he discovered a
server that could be used by would-be attackers to get into portions of the
Excite@Home corporate network. Among the accessible data was a customer
support database of users, their machine configurations and their addresses,
Excite@Home spokeswoman Londonne Corder said.

However, no credit card information was in the database, she stressed, and
because of Lamo's aid, no records were accessed by others. Lamo first found
the network vulnerability in March, she said.

The details of the breach were first reported by security site
SecurityFocus.com, which had been contacted by Lamo.

Lamo is "someone who tries to uncover security holes with good
intentions--to show us where we had some security holes, so those could be
fixed," Corder said.

While not a first, a collaboration like Excite@Home's cooperation with a
hacker to secure its network is rare.

Despite the open-source movement underscoring the historic definition of
hackers as curious--if unconventional--researchers, companies have been

frequently leery of associating with anyone who considers themselves one.

Yet, the Excite@Home network seems a bit more secure today because of the cooperation.

"After meeting with Lamo, we took steps to further secure the corporate network by installing firewalls, restricting access to the network, implementing programs to prevent denial-of-service attacks, and adding hardware and software designed to detect and prevent security breaches," Corder said.

***

Wireless Privacy Legislation Coming
By Doug Brown, Interactive Week
May 28, 2001 5:56 AM ET

Convincing lawmakers that cyberspace needs sweeping privacy regulations hasn't been an easy sell, and lobbyists and partisans on opposing sides in the debate have dug trenches and settled in for a long policy slugfest.

Privacy, it turns out, is simply complicated.

But for privacy advocates, there is hope that in one electronic environment - wireless - legislation could come sooner rather than later. Senators John Edwards, D-N.C., and Byron Dorgan, D-N.D., plan to offer the first legislative salvo in the wireless privacy debate sometime after the Memorial Day recess, which ends June 3, according to an Edwards staff member.

The bill, the staff member said, will address the privacy of location information, data that has the potential to shower marketers with new selling channels but at the same time could easily infuriate consumers and lead to much tougher legislation.

Because of a 1999 amendment to a bill, cell phones now must be equipped with technologies that reveal to law enforcement officials the locations of cellular phones during 911 calls. Among other things, the bill did forbid cellular carriers, which have access to this location information, from using it in any way without the explicit consent of individual cell phone

users.

But as web-enabled personal digital assistants (PDAs) and cell phones merge into single devices and carry location-driven applications - such as services, for example, that will flash advertisements on a PDA when users pass stores having sales, or services that alert users to traffic conditions - privacy advocates are eager to make sure that this information cannot be freely distributed. The 911 amendment applies to wireless carriers, but it does not necessarily address applications providers.

"The question is, what are the rules for these applications," said Ari Schwartz, a senior policy analyst at the Center for Democracy and Technology, a cyberspace civil liberties organization. "And most importantly, what are the rules for government and for civil cases? Imagine a civil case is brought against you and they have everywhere you have been. The technology becomes a dog tag."

Schwartz said the legislative proposals to be aired in coming months will attempt to "level the playing field" between the wireless carriers and the application providers, so, for example, just like wireless carriers, application providers would have to get the consent of consumers before they tracks their locations.

The wireless industry has not tried to block legislation that would require application providers get consumer consent before they track them or trade in the location information. Schwartz praised the wireless industry for recognizing that location information could be particularly sensitive to consumers.

Phone spam, for example, could become a major problem without legislative remedies.

"If it's cheap for application providers to have the phones of thousands of people to ring, they will do it," he said, if only for a single sale.

The industry has always been supportive of a restrictive "opt-in" scheme. That's where consumers must offer explicit consent before companies can use their personal information. "It's in the carriers interest to have customers carrying their phones and having their phones turned on," said Michael Altschul, general counsel and vice president for regulatory policy and law

at the Cellular Telecommunications and Internet Association. "Carriers will be sensitive to spam." Altschul said the industry backed the 911 amendment, which forced the "opt-in" embrace.

The debate about privacy, he said, is just starting to heat up now because most of the services that would take advantage of location information haven't been deployed yet. The industry has been involved with the larger online privacy debate, in which those advocating "opt-in" and those backing "opt-out" regulatory regimes are at odds, mainly to make sure that regulations that might make sense for computers - but not necessarily cell phones - don't apply to cell phones.

"So when people are talking about various requirement and scrolling notices, they recognize that unique differences that wireless and wireline devices have," Altschul said. "A privacy statement on an opening screen, if you are using a handheld device, is not an efficient or satisfactory way for the consumer or the industry to provide notice of privacy."

***

(for internal use only)

* * * * * * * * *

WorldCom Public Relations

b6 -5
b7C -5

Date: <u>Mon, 28 Apr 2003 14:40:17 -0400</u>
From:
Subject: Internet Policy News
To:
Reply-to:
X-Mailer:
Importance: Normal

b6 -5
b7C -5

***

1. A New Way to Catch a Hacker
2. Blacklisted E-Mailers Sue Anti-Spam Groups
3. Internet pioneer discourages legislation to curb spam
***

New York Times 4.28.03

A New Way to Catch a Hacker

By NICHOLAS THOMPSON

For a computer security professional, Lance Spitzner has an unusual goal: He
wants ill-intentioned hackers to steal more Social Security numbers and
medical records.

Mr. Spitzner, a former Army officer, spends his days working at Sun
Microsystems and his evenings running the volunteer Honeynet Project, a
group of security professionals working to track hackers. Until recently,
the four-year-old nonprofit effort focused on building and monitoring
honeypots — computer systems designed to be easily penetrated so that
Honeynet volunteers can covertly scrutinize hackers' tricks when they break
into the systems.

Now Mr. Spitzner, 32, is focusing his efforts on a different type of defense
based on the insertion of "honeytokens" into real databases and systems.

Honeytokens are pieces of seemingly enticing information that have no useful
value. Embedded in ways so that no innocent person should accidentally
stumble upon them, honeytokens trigger alarms when viewed, grabbed or
downloaded. For example, a bank could insert a fake credit card number into
its files and then set up a program called a "sniffer" on the network that

b6 -5
b7C -5

Printed for

would send out an alarm if anyone touched that particular number.

The term "honeytokens" was coined on Feb. 21 by a programmer named Augusto Paes de Barros who used it in an e-mail message to a list of security professionals. But the idea is not new.

It dates back in computing at least to 1986, when Clifford Stoll, a programmer at Lawrence Berkeley National Laboratory in California, buried fake records for an organization called the Strategic Defense Initiative Network deep in his server. When intruders started downloading the records, and then someone sent a letter to Mr. Stoll about the phony organization, he and federal investigators traced the intruders to East German and Soviet intelligence agencies.

Today, the use of honeytokens is not uncommon. For example, ForeScout Technologies, based in San Mateo, Calif., has built a commercial software program that tracks incidents of surreptitious reconnaissance, like port scans — the computer equivalent of someone turning your doorknob to see if it is unlocked. The program will announce a false message of vulnerability to the scanner in the form of a honeytoken. It then breaks the connection if the hacker follows up with an attack.

Honeytokens, like their cousins the honeypots, are based on the notion that if you build it, they will come. Mr. Spitzner became intrigued by the idea of honeypots after putting a new computer online at home and watching it get attacked within 15 minutes by an automatic program scanning the Internet for vulnerable prey.

Many computer criminals break into systems simply for the fun and challenge. Others are looking to take over vulnerable systems in order to use them as safe houses for setting off further, more serious, attacks. Others want to mine credit card addresses or steal corporate secrets. According to a 2002 report by the Computer Security Institute, 90 percent of the 500 corporations, government agencies, financial institutions, medical institutions and universities surveyed detected security breaches during the previous year.

Honeytokens could also be useful for national security purposes. Michael Vatis, director of the Institute for Security Technology Studies at Dartmouth University, said that the Defense Department could use them to

snare people seeking unauthorized information on weapons systems. For example, a honeytoken could be designed so that if it were downloaded and then taken to a different system, it would be able to contact its original server each time it was accessed. One way to do this would be to include code in the honeytoken that would automatically try to fetch a tiny image or some other file based on the home server, making the honeytoken "phone home" whenever it is opened.

Honeytokens also can be used to track attacks from within a company by people who have passwords to enter the system legitimately. Pete Herzog, managing director of the Institute for Security and Open Methodologies, says that he has used honeytokens to detect when employees illicitly download forbidden material. For example, he has entered corporate memos with particular typos into private databases and then monitored company networks to see where those typos show up. Tracing these honeytokens, he says, often leads to caches of illegal materials stored on the network.

No one believes that honeytokens can stop all cybercrime. But they could offer an upgrade in protection.

Honeytokens offer another advantage: They help reduce the number of false positives in other cyberdefense systems. Like car alarms, intrusion detection systems can go off so frequently because of accidental trespassing that many security administrators ignore the warnings. Honeytokens, if designed correctly, should trigger alarms only if there is a malicious attack.

Hackers, however, are not impressed. Adrian Lamo, who gained notoriety last year when he claimed to have broken into the systems of a number of companies, including Yahoo, says he is not worried. "It's a form of old-school security," he says. "It will work on the people who have been to the old schools."

Mr. Lamo says that he only goes after information that he knows other people frequently seek access to and that he runs credit checks to ensure that information he uncovers, like Social Security numbers, are real. Mr. Spitzner contends that it should not matter whether a hacker bothers to run a credit check because the alarm should ring any time the decoy record is accessed.

Hackers can also evade honeytokens by compressing and password-protecting
the information they steal, thereby changing or hiding the data, like fake
Social Security numbers or typos, in memos that the sniffers are searching
for. And "phone home" honeytokens designed to trace users could be thwarted
if opened only on computers disconnected from the Internet.

Some experts are also worried about the possibility that using honeytokens
could violate the federal Wiretap Act, which places limits on intercepting
and monitoring electronic communications. Richard Salgado, senior counsel
for the Justice Department's computer crime and intellectual property unit,
has said that very little law governs this new area and that security
technicians should consult first their lawyers.

Mr. Spitzner said that he was less worried about the law than about smart
hackers. Honeytokens cannot solve all problems, he said. "But they can make
a very simple and powerful tool in a security arsenal."

*****

Washington Post, Saturday, April 26, 2003; Page E01

Blacklisted E-Mailers Sue Anti-Spam Groups

By Jonathan Krim, Washington Post Staff Writer

A recently formed group of e-mail marketers has opened a new front in the
escalating war over unsolicited e-mail, suing several organizations that
track and "blacklist" alleged spammers so that their messages will be
rejected by Internet service networks.

EMarketersAmerica.org, a nonprofit Florida corporation, charges that
spam-tracking groups falsely accuse legitimate marketers of being spammers
and ruin their businesses by blacklisting and harassing them.

The tracking groups, which include Spews.org and Spamhaus.org, keep
databases of information about accused spammers, publishing as much personal
information about them as is available.

b6 -2,5
b7C -2,5

To:
From:
Subject: Fwd: Hacker Story
Cc:
Bcc:
Attached:

forwarded this to me.

=============================

MCI Security Hole Put AOL, Others, In Hacker's Crosshairs

By Brian Krebs, Newsbytes
WASHINGTON, D.C., U.S.A.,
05 Dec 2001, 2:10 PM CST
MCI WorldCom [NASDAQ:MCIT] recently moved to secure several vulnerable portions of their network that allowed a researcher to obtain the keys to private network routers for dozens of Fortune 500 companies.

AOL Time Warner, Bank of America, Citicorp, Fox News Corp., JP Morgan, McDonald s, and Sun Microsystems - to name just a few - were among those firms whose internal systems information was vulnerable to compromise.

Security researcher Adrian Lamo discovered the vulnerability after stumbling upon several proxy Web servers on MCI's Internet address space. The proxy allowed Lamo to gain access to the company's Intranet, and to a tool that MCI technicians use to perform routine router maintenance for hundreds of the company's largest customers.

After realizing the full extent of the information and access at hand, Lamo contacted WorldCom through security intelligence firm SecurityFocus.com.

Not only did the security hole allow Lamo to remotely manage customer routers, this vector paved the way to customer access information including router dialups, logins, and "enable" passwords - the administrative passwords needed to take total control of a router.

Printed for

1   b6 -5
b7C -5

Such information could allow an intruder to divert network traffic for any of the affected companies, or disable their networks altogether. In contrast to most networks, which are routed publicly over the Internet, these customer networks were fully internal, running over private lines and address space, sometimes connecting corporate offices across coasts or continents.

"It would have been pretty trivial to reset the password on any of these routers, which would have made it impossible for companies to perform remote maintenance on them," Lamo said in an interview with Newsbytes.

"That would effectively paralyze many of the companies dependent on their network infrastructure, because support staff would have to be dispatched to reset each router's information via a live hardware procedure. It could have been a real nightmare for some of the biggest players in the U.S. economy."

The Web tool also included dial-up numbers and user/password information for routers serving dozens of other major companies - both domestically and abroad - including British Airways, Clorox, Daimler Chrysler, Dow Jones, the U.S. Department of Interior, the U.S. National Park Service, Ford Motor Co., Frito Lay, the Home Shopping Network, Nintendo and Pfizer.

MCI Spokeswoman Jennifer Baker said the company is grateful that Lamo opted to work with them over the weekend to correct the problem.

"We learned on Friday that unauthorized access could be made to our administrative internal data network, a network that employees use to access MCI intranet sites," Baker said. "We immediately investigated the issue and corrected it and made sure no Worldcom customers were affected, and we certainly appreciated Adrian working with us so cooperatively over the weekend."

Once on MCI's corporate intranet, the 20-year-old hacker was able to deconstruct most of the checks and balances that prevent the average employee from manipulating accounts and procedures on the network. Over time, he was able to make management-level decisions in various automated processes, such as creating, viewing and deleting employee records.

"Using that information, an intruder could have intercepted and redirected e-mail for almost all employees, right up to the CEO, and with a bit of forethought changed the direct-deposit settings for any number of employees so that their paycheck ends up in an account in the Ukraine," said Lamo, who provided Newsbytes with a set of partially redacted screenshots to document his tracks.

"They had some very good precautions and fail-safes in place, but ultimately they were faced with an extraordinary situation that was never designed for someone sitting at Kinko's for a solid day looking at every angle he could think of," he said.

Also buried within MCI's intranet was basic account information for other entities, including data and dial-up service accounts for the intelligence agencies, the MPAA, the Church of Scientology, and similarly diverse customers.

The availability of such data raises chilling possibilities at a time when U.S. federal law

b6 -5
b7C -5

enforcement agencies have expressed growing concern that a cyber-attack on the nation's most important computer systems could accompany the next terrorist strike.

"When you have a company that many of the major players in US business rely on for critical services, it is beyond essential that sensitive information of this caliber be available only to those with a genuine business need for it," Lamo added. "I started with the same level of access as any employee. The newest intern could have done the same thing.

"Thankfully, WorldCom's response was extremely prompt and effective, reflecting their level of concern in addressing these issues. Many of the points raised are not WorldCom-specific - you see these patterns at countless companies of this size."

MCI is the latest in a string of companies Lamo has found to be vulnerable to Web-based intrusion. Days after the Sept. 11 attacks, Lamo used a proxy on the Yahoo network to add satirical content to a story on the company's Web site about Russian programmer Dmitry Sklyarov, a stunt that raised public concern about the integrity of online media.

Earlier this summer, Lamo alerted ExciteAtHome to similar vulnerabilities on the company's network that left the personal information of nearly 3 million customers and several thousand company employees available to even the most marginal of system crackers. ExciteAtHome later thanked Lamo for helping them to patch the hole. Lamo has also highlighted related vulnerabilities at Microsoft and America Online.

Lamo said most companies are so concerned about protecting their networks against typical cracker exploits - such as common software bugs and buffer overflows - that they typically overlook security on internal Web-based systems designed solely for use by employees.

"Companies don't generally pursue this angle of insecurity, and tend not to consider that confidential resources might be available to anyone with a Web browser," he said. "Many of these companies are running intrusion detection systems that will trip alarms if they spot someone scanning for known exploits. But most often, normal Web traffic goes unnoticed."

Reported by Newsbytes.com, http://www.newsbytes.com

Business Markets Public Relations
WorldCom, Inc

b6 -5
b7C -5

Phone
Pager

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ WFO|NVRA _____

Serial # of Originating Document _____

Date Received _____ 9/23/2003 _____

From _____

_____

(Distributor)

_____

(City and State)

By __ SA _____ /SA _____

b3 -2
b6 -1,6
b7C -1,6
b7E -3

To Be Returned   ☐ Yes   ☑ No
Receipt Given   ☐ Yes   ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes   ☑ No

Federal Taxpayer Information (FTI)

☐ Yes   ☑ No

Title: ADRIAN LAMO;
NEW York times—VICTIM;
Computer Intrusion
OO:NY

Reference: _____

(Communication Enclosing Material)

_____

Description: ☑ Original notes re interview of _____

_____ Interview notes _____

b6 -6
b7C -6

FBI(19-cv-1495)-2168

9/23/2003

b6 -1,6
b7C -1,6

ISP-Speakeasy DSL

owned by others.

b6 -6
b7C -6

Ran Conference in
Vegas. DefCon.

on west coast
e-mail communication.
unfrequentl—

often

source d/n think
changed hands
Reports

doesn't host his website

why —
   not intentionally. usually
starts w/ browser, very basic
no technical background

and freedom of thought — homeless

adrian@adrian.org

b6 -6
b7C -6

no drugs while he was

@ _____

has tried some staff

NON disclosures don't like him.

_____

usually concurred.

_____ Similary to

him

Strong sense of morality/
spirituality

does not confide in people

FBI(19-cv-1495)-2173

Served P

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ NYO _____

Serial # of Originating Document _____

Date Received ___ 11/25/03 _____

From ___ Self- generated _____
                        (Name of Contributor)

_____
                        (Address of Contributor)

_____
                        (City and State)

By [_____] _____

To Be Returned   ☐ Yes   ☑ No
Receipt Given   ☐ Yes   ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes   · ☑ No
Federal Taxpayer Information (FTI)
                  ☐ Yes   ☑ No

Title:

Reference: _____
                        (Communication Enclosing Material)
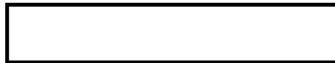
Description: ☐ Original notes re interview of

BACK GROUND CHECKS OF :
① [_____]
②

b3 -2
b6 -1
b7C -1
b7E -3

b6 -3
b7C -3

FD-340a (Rev. 11-12-89)

(Title) _____

(File No.) _____

Item	Date Filed	To be returned			Disposition
		Yes	No		

Full Name: Gary Gygax
Last Name: Gygax
First Name: Gary

Business Address: PO Box 388
Lake Geneva, WI 53147

316 Madison STreet
Lake Geneva, WI 53147

Business: (262) 248-7380

SSN: 387-34-8291
DOB: 1938

☑ Help us decide the next Recognized Variant! ☑

Nine different Chess Variants available to be played On-line!

Person Information

Gary Gygax

ggygax @ genevaonline.com

Well-known RPG game creator Known for Dungeons &Dragons (tm) and DragonChess (tm) among many others.

Items this person authored | Items this person invented

[Edit] | [Search]

This person is not a registered chessvariants.com member. If you are Gary Gygax and wish to become a chessvariants.com member, please press the 'Register' button below. You will be sent an email with your user id and password. Becoming a registered member will allow you to particiapte in various chessvariants.com events such as contests, voting and polling.

Register

GARY GYGAX FAQ

What is happening now?

Let me pick that up from just after TSR sued and we settled the matter of the DANGEROUS JOURNEYS/MUTHUS RPG system.

In 1995 I determined to turn to computer RPGs. Two were successfully optioned. Neither went into actual production. In one case the CEO of the producing company was changed, and the new president wanted to change the contract, even have control of the use of my name! Scratch that deal. The second one we had was near production, we got word that it was moving forward on a Monday, then got a call on the following Wednesday that the company had been sold and all projects not actually in production were canned. Scratch two:(

That did it. Back to the paper game. So that's when work on the LEJENDARY ADVENTURE RPG system commenced in earnest. Those who visited this website in the past likely recall seeing the appha and beta test LA rules posted here for more than two years.

In 1999, at GenCon, the publisher, Hekaforge Productions, released the LEJENDARY RULES FOR ALL PLAYERS in the Author's Signed Edition. In mid-2000 we finally managed to get all three core rules books in all three editions, into print--along with a LM screen and a couple of adventures.

As of now, December 2000, I have written quite a number of works for the game system, some in print, some coming. These are: LEJENDARY RULES FOR ALL PLAYERS, LEJEND MASTER'S LORE, BEASTS OF LEJEND, LEKENDARY EARTH World Setting, LEJENDARY PANTHEONS, KEY OF SAND sourcebook, MALEDICTED Sourcebook, WELL OF SHADOWS (with Jon Creffield) Adventure for MALEDICTED, LEJENDARY ASTEROGUES Fantastical Science Genre Expansion for the LA RPG (LEJEND MASTER'S LORE [two volumes] and LEJENDARY RULES FOR ALL PLAYERS), THE HERMIT Adventure, LIVING THE LEJEND Introductory Adventure Module, and one generic work--"Weyland

Smith & Company GIANT FUN CATALOG of Unsuspected Mirthful Magic
Apparatus, Entertaining Enchanted Items, and Hilarious Heka Objects you MUST
possess."

I am also working on some additional projects for the lines mentioned: For the LA
game line several adventures. For the generic line three books, one dealing with the
criminal underclass in a fantasy world, one dealing with the socio-economic classes
and their everyday life in a fantasy world, and one book of things and facts used for
creating and filling the fantasy environment (the latter with Daniel Cross as co-
author). For the LEJENDARY ASTEROGUES Fantastical Science Genre
Expansion a campaign sourcebook.

Meantime I am the one who reviews and develops/pre-edits all freelance
submissions for new products for the LA RPG system. this includes the line of
fantasy novels set on the LEJENDARY EARTH world that Hekaforge will be
launching soon (likely on early 2001).

Of course I do contract work for Wizards of the Coast, most notably the fairly
regular column, "Up on a Soapbox" appearing in DRAGON Magazine. Add to that
some small amount of freelance writing that's called for now and then, and you will
see I don't lack for things to do...

Finally, yes! I do still manage to play games. I run a regular LA game campaign
each Thursday night. It is about five years old now and going strong. I hope to add
another RPG campaign soon, time permitting. When odd opportunities permit, we
play boardgames, cards, and the like too. What use in being a game designer if one
can't play as well as create?

Back to the top...
Back to the homepage...

AD&D and My Leaving TSR

Many people are under the mistaken impression that Gary Gygax owned the
majority interest in TSR. This is not the case, and here is the chronology that
brought a definite minority shareholder status for Gary:

1973: Gary and Don Kaye form Tactical Studies Rules, an equal partnership.

1974: Brian Blume is admitted as an equal (1/3) partner.

1976: Don dies of a heart attack in January. His wife is impossible to deal with. TSR
Hobbies Inc. is formed, and this corporation buys out Don's widow. At this point,
Gary controls the corporation with c. 60% of the shares. Later on, because of
extreme cash shortages, having spent a lot to buy out Mrs. Kaye, shares of TSR are
sold to Brian and his father, Melvin. By the fall, Gary's interest in the corporation is
down to about 35%, and thereafter it dropped to around 30%.

Simply put, he didn't have the money to keep up with the share purchases. Yes, he

placed his own interests below those of the corporation.

1985: Gary exercises an option, and with what amounted to a handful of shares voted by other family members, he had a c. 50.1% majority. Later, when Brian Blume exercised an option he held, so as to sell those shares, and the others he and his brother Kevin held, to Lorraine Williams, Gary was again a minority shareholder.

In this same year he sued to prevent the transfer of Blume-owned shares, arguing that a corporate buy-sell agreement prevented the sale to Williams. The local judge rules otherwise.

Back to the top...
Back to the homepage...

What Happened to Gygax - TSR?

The reader is referred also to the FAQ regarding stock ownership in TSR, as it explains a good deal of what happened.

Gary was President of TSR Hobbies, Inc. when it was formed in 1976. In fiscal 1981 the company made c. $16.5 million dollars income, with c. $4.25 pre-tax profit. At this time, corporate long-term debt was about equal to an average month's receipts. Gygax did not believe in borrowing money except for short-term needs, for projects that could not otherwise be produced, but that would in a relatively brief time generate sufficient sales to repay any loan needed to get them to market.

The board of directors of TSR then consisted of Gary, Brian Blume, and Kevin Blume. The latter two voted about 60% of the outstanding shares of stock of the corporation, compared to Gary's c. 30%.

The Board decided to reorganize the company. Gary would be president, but "beneath" him were two other presidents: Brian Blume was "President of Creative" at TSR, and Kevin Blume was "President of Operations". In theory, they reported to and took direction from Gary. In reality, being two-thirds of the board, the Blumes ran TSR and Gary was boxed out.

From that point on, Gary never ran the company, and had to fight for anything he thought was in the best interests of TSR. Gary wanted to keep the best quality in binding and products in general. He believed that authors of works should have their names on the works. He believed that some royalty should be paid to creative employees. He thought that all employees of TSR should be able to buy shares of stock and participate in ownership.

All of these ideas were antithetical to the Blumes, it seems. Each of these instituted practices were done away with systematically. with product quality being the main target. Brian Blume stated publicly that he wanted "obscene profits at federally insured safety".

In 1983 Gary was instructed by the board to go out to California and set up TSR Entertainment Corp., a company owned by the Exempt Profit Sharing Plan of TSR. He did so, changing the name of the operation to Dungeons & Dragons Entertainment Corp. after discovering that the entertainment business community there would not do business with TSR.

DDEC had the D&D Cartoon Show and several other fledgling projects underway. It was responsible for the closing of the deal whereby Speilberg licensed the name, AMAZING STORIES, from TSR.

Gary returned to Lake Geneva in the winter of 1984 because T¦ ¦ was in debt and the bank was threatening to force it into bankruptcy. Associates of his called to inform him that Kevin Blume was shopping the company on the street, as is said, out in New York City.

By this time the Blumes had forced him to accept three "outside" directors on the board. The Blumes had embraced the precepts of the now-defunct American Management Association. It was inept at promulgating even manufacturing ideals, in Gary's opinion.

These three petty businessmen, two executives and a lawyer, were absolutely ignorant of the gaming business, and under their direction, and with the Blumes leading the way, TSR had accumulated $1,5 million debt that they couldn't figure out how to pay: amongst their ideas were the dropping of the RPGA and the sale of DRAGON Magazine. After some thought, Gygax presented a long letter to the entire board, outlining the mismanagement of TSR by Kevin Blume, and demanding his resignation and replacement. The board voted four to two, the Blumes abstaining, to remove Kevin and put in place a pro-tem president, one Richard Koenigs. With direction form Gary and other executives of the company, some 90 relatives of the Blumes were removed from the payroll, various corporate owned and leased cars, scores of them, were gotten rid of, unused system office furniture owned and leased was likewise sold or returned, and two major releases were rushed into print--UNEARTHED ARCANA and ORIENTAL ADVENTURES. By April

1985, the corner had been turned, and the American National Bank was no longer glowering and considering pulling the loan plug, so to speak.

It must be noted that the bank was not only not helpful, they were quite obstructive in getting the corporation back on its feet, in Gary's opinion. Prior to the April date, Gygax exercised an option he held, putting many thousands of dollars into the plus side of the corporate ledger, and also assuming a bare majority control thus. He than took the office of the presidency, and told the three "outside" directors that their days were numbered. They had,, he said, "pontificated business" while the company went to near ruin.

Not surprisingly, these three sterling individuals were aligned with Williams and the Blumes in the dispute over whether or not the latter could sell their shares, and an additional 700 they secretly purchased by option exercise. to thus allow Lorraine Williams majority control of TSR.

Learning of the scheme, Gygax acquired attorneys and managed to have a temporary injunction granted so as to prevent the share transfer. However, in late 1985 the county judge, who seemed unable to recognize what constituted a contract, as Gary says, decided in favor of the defendants. At this juncture Gygax started an appeal, but was both hard pressed for funds and heartily sick and tired of the mess. Just before the end of the year, Gygax agreed to sell his shares and other interests to TSR, and left the corporation in the hands of Williams.

The capacity of Lorraine Williams to manage a game company is no longer in question. With a debt load of perhaps $30 million dollars or more, and facing bankruptcy soon, she sold out to Wizards of the Coast in 1997. That is surely a step in the right direction for TSR. Gary believes. Williams despised gamers, and she stated in his presence that they were not her

"social equals": She also claimed she was going to show the game industry how business should be conducted. Some lesson.

Clearly, Wizards of the Coast is not of that ilk, runs an excellent operation, and under their direction TSR fans should see a major improvement.

Back to the top...
Back to the homepage...

What Happened to the D&D Movie?

Even before the cartoon show was in production, there was tremendous interest from Hollywood in producing a movie based on AD&D. Gary was active in working with various agents and would-be producers and studios with an aim towards making a movie deal actuality.

The story is lengthy, but the meat of it is this:

A script from James Goldman was acquired by TSR. Several tudios were interested. Gary did all he could to get a major theatrical motion picture into production. Every proposal was vetoed by the Blumes and/or TSR board of directors.

Gary had a meeting one morning with Sid Shineberg, then president of Universal. Mr. Shineberg said to Gygax, when Gary came out and asked exactly what his interest was, "We want to acquire you (TSR), joint venture with you, or do just about anything you would like in the way of getting a motion picture deal done."

Shaking his head sadly, Gary told Mr. Shineberg that as a minority shareholder in a closely held corporation, he could only recommend. No trouble guessing what the reaction of Brian and Kevin Blume was to that so that offer ignored, and all others scotched by demands that were impossible, no film contract was ever signed.

That, incidentally, pretty much spelled the doom of DDEC--Dungeons & Dragons Entertainment Corp., of which Gary was then president. However ...

Dangerous Journeys / Mythus

This multi-genre game system and the first game within it, the MYTHUS FRPG, were conceived in 1986, when New Infinities was in operation.

Gary began writing a horror-based RPG then, and his son, Luke was the first play-tester. After NIPI went down the tubes, he collaborated with Mike McCulley. Mike was co-author of the whole underlying game system, although he hasn't ever gotten proper credit, because of later events.

When large computer corporations were involved via the offices of two agents then representing the game system, it was decided that fantasy rather than horror must be the initial release in the DJ line.

Dave Newton was contracted by Trigee to co-write the now-rush MYTHUS FRPG. So work began immediately, and Game Designers' Workshop was signed up as publisher of the paper side of the game.

The rest is history that's pretty well known. TSR sued claiming all sorts of things, but going mainly on copyright infringement. The suit was settled. TSR paid certain considerable sums of money (in addition to the c. $2 million they had tossed to their lawyers to suppress the game), and they acquired DJ and the ancillary things such as JOURNEYS and MYTHIC MASTERS Magazines.

As of June 1997, there is no indication that DJ will ever be revived, although there is considerable following, and also some "expansion" of the system with enthusiast-generated additions and rules for personal use by active groups so as to be able to continue play in other genres, Gary is told.

To the best of his knowledge and belief, the suit was not the proximate cause of the eventual demise of GDW. In fact, under the settlement, they paid none of the legal fees for defense against TSR's claims, and TSR purchased remaining inventory from GDW.

New Infinities

Gary was never an employee of New Infinities Productions, Inc. He was a big investor, and a member of the board, but he did not hold any office in the corporation.

The one who formed it assured Gary that venture capital to the tune of up to $2 million was available. With credentials including the Wharton School of Business, and face-to-face meetings with attorneys, accounts, and banks--and a seemingly

barely-missed meeting with the investment people. Gary agreed.

The end of the tale is that there were never any venture capitalists on tap, it seems. When a demand was made to bring the money in, Forest Baker tendered his resignation and in no time NIPI was down the tubes.

Gary was the major investor, and he lost by far the greatest amount of money in the deal. However, he apologizes to all the others who, on the strength of his participation likewise invested and lost money in the concern. It was a matter of too many people taking large salaries out of NIPI while product was lacking to support such excess.

Had Gary been able to write about ten times faster, then perhaps it would have succeeded. As it was, the five Gord the Rogue books were all paperback best sellers on the B Dalton and/or Waldenbooks lists, but it wasn't enough. Royalties due were also mostly not paid.

Back to the top...
Back to the homepage...

Divorce/Sales of Stock by Ex-Wife

Yes indeed. At the same time Gary was attempting to prevent the sale by Brian and Kevin Blume of controlling interest shares of TSR to Lorraine Williams, he was in the middle of a divorce.

It is true that his now ex-wife did plan to demand half of his stock holdings in the divorce, and as she was so doing she was in contact with Williams, attempting to get her to agree to buy them at a very high price.

That is more than enough about that. Talk about wretches!

Back to the top...
Back to the homepage...

RPGnet

A library of articles about Online Games

Industry Insights: The RPGnet Interviews

Interview with Gary Gygax, part 1 of 3

by Scott Lynch
May 1, 2001

Editor's Introduction
I selected Mr Gygax as my first interview subject for four major reasons

1 Name recognition, baby,

2 I knew that mentioning his name in my intro piece would generate a flurry of comments, and I really wanted to see what the reaction of readers would be,

3 Gygax is now 62, and speaking frankly he's not going to be around forever, and

4 While surfing various interviews and web commentaries on gygax and his work I became a armed at the general acceptance of rumor and hearsay governing his reputation Gygax-trashing' was a widespread pastime It was taken for granted that he was a 'dinosaur that he was

Birthplace: Chicago, Illinois
Date of Birth: July 27, 1938
Current Residence: Lake Geneva Wisconsin
Immediate Family: Wife Gail, son Alex at home six other children grown and on their own Ernie, Elise Heidi, Cindy, and Luke
Pet: One cat, Nema
Favorite Book(s): Too many to possibly list here' Jack Vance is my favorite author in general, though
Favorite Films: Lots of these- ranging from *The Third Man* and *The Deep, Enter the Dragon,* and *The Seven Samurai* and including *The Longest Day, Alien,* and *Zardoz* I know I've missed at least two, but
Favorite Musicians: I listen mostly to classical, Spanish guitar, jazz and some blues too Of composers, I am drawn to Mozart and Beethoven Segovia surely was master of the guitar, and the "modern" jazz musicians are my favorites-- Parker, Davis, Gillespie Hinton, Rich Anita O'Day, Billie Holliday, Stan Kenton-- all that lot As to blues well all the 1940s and 50s performers are fine by me, from Joe Turner and BB King to Leadbelly and Big Momma Thornton
Favorite Beverages: Coffee in the AM, iced tea a Gibson before dinner, a good Bordeaux with that meal, Armagnac after A cool glass of ale (Samuel Adams is fine) just about anytime in between
Favorite Foods: Most any from the top cuisines- (Northern) Italian topping the list, then Chinese, French

no longer "relevant."

I pondered what it meant to be "relevant" as I composed my solicitation letter to Mr Gygax in November of last year. Several associates warned me that he was a crotchety old throwback to the Paleolithic era who would bite my head off as soon as throw a sharp glance in my direction. To my surprise, he agreed to a pretty rigorous interrogation and even wound up inviting me to stop by if I ever pass through Lake Geneva.

I completed a 39-question interview with him and whittled a few dull and superfluous questions out The final draft was just a little under 10,000 words, divided into three sections. Although the early portion of the interview clearly reveals that this is my first time doing any such thing, I believe that the affair became much more lively as it evolved and I gained a little confidence in my job.

and Hungarian. I like to be a gastronome when I'm somewhere that there are better restaurants. Not much in that vein hereabouts...
Other Interests: You mean besides gaming and my family? Football, history, and fishing when I can get away from work likely top the list. Seems there's so much to be interested in it's hard to pin down.

RPGNet: You've been active in the gaming industry for three decades now. Why should anyone still care what Gary Gygax has to say about anything?

Gary: If I were a sports figure, I would agree that age might affect performance.

While I might say that seeing that Beethoven wrote eight symphonies over many years of time, and why be interested in a ninth one, I'll refrain. As it is, I believe that after more than 30 years as a game hobbyist, fan, and author, the experience gained over those many years enables me to bring something new and different to the table with each successive design

In short, no "Johnny One-Note" me!

As an aside, there is also a certain repute that is attached to the "Gary Gygax" whatever. Now, a few think it less than sterling. From where I sit, recalling a standing ovation from a packed audience at GenCon 32 (even though that made me quite uncomfortable, it really impressed me), the press I get, the thousands of communications I receive thanking me for my work, the answer to the last part of your query is pretty easy to answer. If someone doesn't care what I have to say about something, I'll sic my fans on 'em!

RPGNet: So, just how long and hard are you working at 62, in contrast with yourself at 50 or at 40?

Gary: There is no difference in the time I put into game-related work now, in my 60s, than that of my 50s or even 40s. Of course, now I am spending more time with e-mail than I did back then managing business matters. In fact, I have to fight to get time to do research these days, something that in past times was not so much a problem.

RPGNet: What are the contents of one of your typical workdays?

Gary: My usual workday here begins sometime around 6 AM, maybe 7 AM or so if there's something particularly interesting on C-Span. Then I work on through until around 6 PM or so, usually a bit later if I start later than 6 AM The exception is on Thursday, RPG campaign day! Then I close down at 5, eat an early dinner, and am ready to play by 6:30 in the evening.

By the way, I keep that schedule at least six days a week, sometimes seven, but not during football season.

RPGNet: And where does all that effort go? What projects are in the oven for you in the next twelve months or so?

GARY: Whew! That's a tall order, and I'll have to guess at it a bit, because the release schedule is a bit fluid. Here goes in regards to *major* work only·

Awaiting release, in likely order of publication:

Lejendary Adventure, Lejendary Earth World Setting;
*Key of Sand,*Lejendary Earth sourcebook;
*Lejendary Pantheons*sourcebook,
*Maledicted,*Lejendary Earth sourcebook;
*Well of Shadows,*Maledicted adventure;
*The Hermit,*adventure;

For a yet untitled generic line of GM-aid books, possibly "Gygaxian Fantasy:"

The Weyland Smith Catalogue("Joke" magic items);

In final stages·of polish before being turned over for editing:

LA Game *Lejendary Asterogues*Rules, genre expansion;
ditto Lejend Master's books, 2 volumes;

For a that as-yet untitled generic line of GM-aid books:

The Canting Crew;

In process of design, near completion:

*Lejendary Asterogues*Kowloon Wharf sourcebook and adventure;

Working projects

For that as-yet untitled generic line of GM-aid books:

Everyday Life in a Fantasy World;
Fantastic Facts & Things Lists(with Daniel H. Cross);
*Lejendary Adventure: Lost Island Sourcebook*and adventure (with co-designers);
ditto*The Emerald Dome*adventure.

That's it

RPGNet: Ack.

Gary: Of course this ignores various short projects such as the monthly essay for the *Dragon,*Magazine column, an adventure that will be coming soon in*Game Trade*magazine from Alliance Distributors, an introduction to a great D20 fantasy product that Swords & Sorcery Studios will release this year, etc. The same with a few other things such as my editorial and development work on the freelance submissions that come in to Hekaforge, and my work on the line of special adventure modules we are in process of creating and publishing for LA game fans who will use them in giving in-store demos- a line of special, short adventures not commercially available.

RPGNet: Do you have any high-tech pipe dreams for the next few years? Is there an emerging technology or an unreleased technology that you're hungry to put to use in some never-before-seen format? Or are you a meat and potatoes man to the last?

Gary: This is a difficult question to answer. I am more a dreamer than a technical guy. Of course I am eagerly awaiting computers that have audio and video capacity so as to make online RPG activity more like a group of RPGers actually meeting in person to play. To me that doesn't seem high-tech at all, just a matter of time.

Currently, I manage to resist getting caught up in computer game play. Knowing I have a great

deal of work do do in a relatively short time, to start playing an electronic game is to kiss that responsibility goodbye. I really do *love* games of this sort, and if I begin, I won't stop playing until I have exhausted the potential of the offering. I have no games at all on my computer, even Solitaire has been trashed from memory All that would just have to go by the boards if a game such as I described above were available. That would be just too much to resist. In fact, the very thought is what keeps me working so hard now- get the creative stuff out, and then I can "retire" and play games instead of designing and developing them.

"I converted a plastic stegosaurus into a pretty fair dragon, as there were no models of them around in those days."

RPGNet: Let's chat a bit about that little fantasy RPG you were involved with. *Dungeons & Dragons* is said to have evolved from a set of medieval miniature rules called *Chainmail*. What, exactly, was *Chainmail?* Was it a commercial project that enjoyed a fair print run, or was it a hobby project that evolved around a local audience?

Gary: Back in around 1968, Jeff Perren became a member of the Lake Geneva Tactical Studies Association. He brought his 1:20 (one figure on the table equals 20 men) medieval military miniatures rules to us, rules he had written mainly for use with his Hauser Elastolin 40 mm figurines. As I happened to be a fan of the period and the figures, what a boon that was! It didn't hurt that I really liked Jeff's rules too. With his permission, I expanded his two pages to a longer treatment, and those were published around 1969 in the IFW's monthly magazine as the "LGTSA Medieval Military Miniatures Rules."

That was just the beginning of things, of course. Because I was, and am still, a great medieval history and gaming buff, I added more to the original base. First I did a little "Jousting" rules set, next added a "Man-for-Man" section to the work, that being a new rules treatment for when one figure on the table represented one man in combat, not 20. The LGTSA then played a lot of such games on the weekend-long game sessions held in my basement where the big sand table stood.

Not long after that, as the members began to get tired of medieval games, and I wasn't, I decided to add fantasy elements to the mix, such as a dragon that had a fire-breath weapon a "hero" that was worth four normal warriors, a wizard who could cast fireballs (the range and hit diameter of a large catapult) and lightning bolts (the range and hit area of a cannon), and so forth I converted a plastic stegosaurus into a pretty fair dragon, as there were no models of them around in those days. A 70 mm Elastolin Viking figure, with doll's hair glued to its head, and a club made from a kitchen match and auto body putty, and painted in shades of blue for skin color made a fearsome giant figure. I haunted the dime stores looking for potential additions and eventually found figures to represent ogres, elementals, etc. The players *loved* the new game, and soon we had twenty or more players showing up for every session

Guidon Games hired me as its Editor-in-Chief for a new game rules and games line it was about to publish. I put all of the rules mentioned above together into a single book, named it *Chainmail,* and it was published by Guidon in 1971. As far as I know, *Chainmail* was the best-selling product that Guidon had. Guidon went out of business in 1974, and at that time TSR acquired the rights to *Chainmail.* TSR published it for several years, from around 1975 through 1978 or so.

"When my youngest daughter, Cindy, added her

eager approval to the combination of "Dungeon" and "Dragon," that confirmed my choice..."

RPGNet: You and Dave Arneson are both generally lauded as the "creators of *Dungeons & Dragons*"yet clear reference to the role you each played in its genesis is hard to come by. Arneson's website, www.castleblackmoor.com, states that Arneson conceived of a proto-roleplaying campaign set in a place called Castle Blackmoor, using a modified form of your *Chainmail*rules, and was invited to Lake Geneva in 1972 to demonstrate it for you and some friends.

Gary: That's essentially correct Dave was running a campaign using the *Chainmail*rules, a variant that sounded fascinating. So he and Dave Megary came down from the Twin Cities to my place in Lake Geneva to do some gaming. Dave Megary brought his game, *Dungeon!* for me to have a look at.

RPGNet: Arneson further says that a correspondence grew between the two of you in the wake of that visit, and you reworked Arneson's reworking of your own rules into what would eventually become *Dungeons & Dragons.* If your account and Dave's account are merged, it seems that you evolved the heroic fantasy battle game from *Chainmail,* he evolved the small-party exploration game from the same rules, and the two flavors bled together with a heavy re-write of existing rules to become *Dungeons & Dragons.* Is this an accurate chronology of events as you remember them?

Gary: Well sorta...

Dave Arneson and I had already been working on various miniatures rules, such as the *Don't Give Up the Ship*rules (Arneson, Gygax, and Carr) that were eventually published by Tactical Studies Rules. We made contact by mail, then personally at a GenCon before his visit to Lake Geneva. Between Dave Arneson's modifications of the *Chainmail*Fantasy Supplement figures, giving "Heroes" four hit dice rather than requiring four simultaneous hits to kill them, and "Superheroes" eight hit dice, and Dave Megary's boardgame based on a dungeon adventure with *Chainmail*"Wizard", "Superhero", "Hero", and "Elf" competing, exploring, slaying monsters, and gaining treasure by so doing, the special nature of what could be done with the rules bases became evident to me.

Dave Arneson never did furnish any solid rules for me to use in devising a new game, although he (and collaterally Dave Megary) certainly did provide solid ideas though. So, as Dave Arneson has said in an interview that was published in *Different Worlds*magazine (#3), I devised and wrote the whole of the work that became the *Dungeons & Dragons*game.

The initial draft was only 50 pages long, written and mailed out to about two dozen fellow members of the International Federation of Wargaming in the late winter of 1972. Thereafter, as play-testing in Lake Geneva proceeded (at a happily furious pace), and responses from the first draft recipients came pouring in, I revised and expanded the manuscript to 150 pages in length. That's essentially what was published in 1974 as the three D&D game booklets.

As an aside, I must laugh at some comment I saw about the name for the game being "The Fantasy Game" until someone "wised me up". Having been employed as an Editor-in-Chief, selecting what game rules and games would be published by Guidon Games since the beginning of 1971, I was well aware of the need to use a working title, the need for some caution in regards using the actual name for a a projected game release. So that's the reason for that bland one on the draft works.

By the time the second draft was circulating amongst the testers, I had decided upon the actual title to be used, D&D. This was done by making a list of likely words. I then asked the members of my gaming group, and my family, to choose that one, or that combination of words, that they found best suited the game, and appealed most. When my youngest daughter, Cindy, added her eager approval to the combination of "Dungeon" and "Dragon," that confirmed my choice, and

that of most of the others too. So the *Dungeons & Dragons* title was born. (As the creator of the IFWs Castle & Crusade Society, I was pleased.

"As for competition for D&D, there was never any serious competitor. For a fact, there still isn't a real competitor for the new D&D, including my own new fantasy RPG..."

RPGNet: Can you tell us anything about developments in roleplaying after 1973-74 that branched out from the magical fantasy roots you and your contemporaries put down? When did your own associates start to experiment with, say, science fiction or western settings? And when did such efforts start to reach commercial publication at TSR and other companies?

Gary: Whew! Another multi-part question. Think I'd better break it up into manageable chunks:

The D&D game was released in January of 1974. By then Don Kaye and I were "noodling" about a Western RPG, for he was a big fan of that genre. Sadly, Don died in January of 1976 Brian Blume took over for Don, and so the *Boot Hill* game was authored thus, Blume and Gygax. So, to the root of the question, that *began* development early in 1974.

Around 1975 M.A.R, Barker sent us the manuscript for his *Empire of the Petal Throne* RPG, the rules inspired by those for D&D, of course. It was a most compelling environment, and we soon published it. Around this same time Brian Blume and I began working on *Warriors of Mars,* a sort of "Barsoomian" fantasy-science RPG It too was published by TSR, but then because of pressure from the Burroughs' Estate the product was not reprinted.

I believe that it was 1975 when the Game Designer's Workshop RP game, *En Garde,* was published. That, to my knowledge, was the first of competing RPGs Most of us at TSR purchased and played it, too. Then, as time passed, *Star Frontiers, Metamorphosis Alpha* (one of my very favorite RPGs, later revised and released as *Gamma World), Gangbusters,* and *Top Secret* (in that order I think) were released by TSR. I assisted in development and/or play-testing with all of those titles.

As for competition for D&D, there was never any serious competitor. For a fact, there still isn't a real competitor for the new D&D, including my own new fantasy RPG . but maybe in time that will change.

When GDW released *Traveller,* we were all pretty enthused, for we saw it as broadening the interest for the RPG by covering science fiction. On the release dates of other companies' RPG, I am not a reliable source- I'm barely that for most of the TSR line other than D&D. What copies of the old products I have, and that's astonishingly few, are sealed away for posterity, so I can't check the copyright dates. Sorry.

Next: The memory of Donald Kaye, fantasy archetypes, and game design philosophy.

What do you think?

Go to forum!

Topics	Author	Date	Latest R
American roleplayers (1) new	Rockwell	05-30-2002 05:08	05-30-20
Re-release is good (2) new	Blu	05-23-2002 12:38	05-24-20
Nice interview. (3) new	Greg Basich	04-24-2002 09 12	08-24-20
Thanks, Gareth. (1) new	Keith Burkhead	04-24-2002 08 14	04-24-20
Spot on! (1) new	Matt M	04-20-2002 04:48	04-20-20
Very nice work (7) new	Steve D	04-19-2002 04 31	04-23-20
Dejavu (1) new	Scarecrow	04-19-2002 01:31	04-19-20
I hate game fiction too (1) new	Phill Calle	04-18-2002 20:10	04-18-20
Great job! (1) new	Cedric Chin	03-31-2002 17:08	03-31-20
That, and $1.298, will get ya a cuppa (14) new	Sam Chupp	03-28-2002 06:46	04-24-20
Amuse me some more! (1) new	KC	03-28-2002 02:34	03-28-20
Marketing (4) new	Ken Burnside	03-27-2002 05:44	03-28-20
Freeport Crisis (4) new	KC	03-24-2002 01:26	03-28-20
What about the rest..? (2) new	Adam Williams	03-23-2002 19:42	03-24-20
What do I think? (5) new	Chris Camfield	03-23-2002 08.15	03-25-20
Only on RPGnet.... (5) new	Gareth-Michael Skarka	02-12-2002 09:08	03-26-20
An Interview (4) new	Dan	02-11-2002 13:56	03-24-20
That was really ... (9) new	S. John Ross	02-08-2002 21:06	02-12-20
Tim Powers? Where?? (7) new	Valandil	01-20-2002 23 39	05-30-20
Catch22 (1) new	Rusty	01-20-2002 20.19	01-20-20
Tim Powers and Unknown Armies (4) new	Mitch	01-19-2002 10:43	09-27-20
The problems I can see... (7) new	Mark Green	01-04-2002 04:33	01-10-20
You know what's a cool thing to put on web pages? (6) new	Jeff Freeman	12-09-2001 02:41	01-04-20
Credit Where Its Due (5) new	Chris Pramas	12-05-2001 15 05	12-05-20
Acceptance Speech [Plus] (3) new	S. John Ross	12-05-2001 12:31	12-07-20
Cool! (1) new	Chris Camfield	12-05-2001 12.18	12-05-20
Heh...now I know why I suck at business... (2) new	Steve D	10-18-2001 01:06	01-22-20
Those wouldn't be _MY_ top 5... (1) new	GAZZA	10-15-2001 01 17	10-15-20
Not to belittle the tragedy... (11) new	Rygar	10-01-2001 08 07	12-07-20
Not sure what to say . . . (1) new	Gordon C. Landis	09-28-2001 00:01	09-28-20

Forum List | Go to Top | New Topic | View Threads | Search   **Newer Messages | Older Messages**

All Industry Insights

- Gareth-Michael Skarka interviews China Mieville, April 24, 2002
- lizard's Condensation of All Game Fiction, April 18, 2002
- Sandy's "God or Whore?" GTS'02, March 26, 2002
- Allan Sugarbaker with GAMA Trade Show '02: An Inside Report, March 22, 2002
- Aldo of Impressions on the GamePlay CD, January 3, 2002
- Gareth-Michael Skarka interviews Ken Hite, February 8, 2002
- Gareth-Michael Skarka interviews Tim Powers, January 18, 2002

- Aldo Ghoizzi on Inside the Making of GamePlay, January 3, 2002
- The RPGnet Awards Cabal presents the RPGnet 2001 Awards Results!, December 5, 2001
- Ken Whitman teaches us with A Note About Creating a Good Promotional Campaign, October 12, 2001
- Sean Jaffe on The Fallout, September 27, 2001 [about 9/11]
- Sean Jaffe on Interesting Times, September 21, 2001 [about 9/11]
- GodLike: Dennis Detwiler and Greg Stolze, September 14, 2001
- Jared Nielsen on Tribe Gamer, August 31, 2001
- Mark Bruno teaches about Copy Editing, August 16, 2001
- Ratings not just kid's stuff for RPG industry, reported by Matt Snyder, August 9, 2001
- GenCon '01 News, reported by Matt Snyder, August 3, 2001
- Origins Report: Would you send your mother to buy from them?, part 4 of 4
- Origins Report: Booth Babes, part 3 of 4
- Origins Report: Overview, part 2 of 4
- The Origins Awards, part 1 of 4, reported by Jason Paul McCartan
- Gary Gygax Interview, part 1 of 3, by Scott Lynch
- Why I Write Gaming Materials by Greg Stolze, November 16, 1999
- Blowing out the Nostalgia Candle by John Wick, October 19, 1999
- Interview with Sean Pat Fannon, *Shards* October 5, 1999
- Portuguese is not Spanish! by Thad Blanchette, September 14, 1999
- Intuition and Surprise by M. J. Young, July 27, 1999
- Fear and Loathing in the Wizards of the Coast Game Center by John Tynes, January 26, 1999
- Breaking In,, on how to break into writing for RPGs, by Steve Kenson, December 22, 1998
- ALT.RPG, first of a series looking deeply at what gaming is all about, by Matt Miller, September 1, 1998
- The Night They Tore Old Mecca Down, GenCon report by Randy Porter, August 20, 1998
- GenCon Fun: con, city, and even housing tips from Randy Porter, June 30, 1998
- GenCon Lore Vol 3: Program Books, update on GenCon 98 attendance, by Randy Porter, June 23, 1998
- The Missing and the Dead, update on GenCon 98 attendance, by Randy Porter, June 2, 1998
- The Definitive Count on who is and isn't attending GenCon 98, by Randy Porter, April 28, 1998
- How to Scam Games Part II by Steve Johnson, March 24, 1998
- The Perils of Penniless Publishing by Aaron Rosenberg, February 3, 1998
- Polyhedral Dice & Mirror Shades, by Greg Costikyan (or, the death of paper).
- Ken Whitman: A Love Hate Relationship by (of course) Ken Whitman
- Interview with Sean Punch, GURPS line editor, by Bob Portnell, October 1997
- YOU DID WHAT? Perspectives On Becoming A Full-Time Writer In The RPG Industry, by Steven Long, September 1997
- A Resurgence of Role Playing, by Gary Gygax, August 1997

Other columns at RPGnet

[Read FAQ | Contact Us]

FD-340 (Rev. 3-8-01)

Universal Case File Number

Field Office Acquiring Evidence   NYO

Serial # of Originating Document _____

Date Received   11/25/03 _____

From   Self- generated _____
                  (Name of Contributor)

                  (Address of Contributor)

                  (City and State)

By

To Be Returned   ☐ Yes   ☑ No

Receipt Given   ☐ Yes   ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

         ☐ Yes   ☑ No

Federal Taxpayer Information (FTI)

         ☐ Yes   ☑ No

Title:

Reference: _____
                (Communication Enclosing Material)

Description: ☐ Original notes re interview of

BACK GROUND CHECKS OF :

b6 -1
b7C -1
b3 -2
b7E -3

b6 -3
b7C -3

Full Name:
Last Name:
First Name:

Home Address:

DOB:
SSN:
CA D/L

Have picture

*Need to do more background

May be related to _____ whose number was called by Lamo

Record Request
FD-125 (Rev. 4-1-93)

RETURN VIA INTER OFFICE MAIL.

Date 04/28/2003

☐ Birth   ☐ Credit   ☒ Criminal   ☐ Death   ☐ INS   ☐ Marriage*   ☒ Motor Vehicle   ☐ Other _____

To	Buded
OPC	

Retur	File number
SA	

Name and aliases of subject, applicant, or employee, and spouse

b3 -2
b6 -1,3
b7C -1,3
b7E -3

Addresses
    Residence

    Business

    Former

*Date and place of marriage
    (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male					
	☐ Female					

Arrest Number	Fingerprint classification	Criminal specialty

Drivers License Number   CA

☐ D/L Photo   ☐ Other

b6 -3
b7C -3

specific information desired

FBI(19-cv-1495)-2332

Full Name:
Last Name:
First Name:

Business Address:

Business:
Home:

SSN:
Owns house

* Someone who knew him was running all his addresses in Lexis/Nexus had to have information about him in order for this to happen, could be he had an ID

Full Name:
Last Name:
First Name:

Business Address:

Business:

SSN:
* SSN is issued to someone who is deceased (possible fraud)
DOB:

Also uses SSN

b6 -1,3
b7C -1,3

65

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ NYO _____

Serial # of Originating Document _____

Date Received ___ 11/25/03 _____

From ___ Self- generated _____
                    (Name of Contributor)

_____
                    (Address of Contributor)

_____
                    (City and State)

By [   ]

To Be Returned   ☐ Yes   ☒ No
Receipt Given   ☐ Yes   ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes   ☒ No
Federal Taxpayer Information (FTI)
                  ☐ Yes   ☒ No

Title:

Reference: _____
                    (Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

BACK GROUND CHECKS OF :

Full Name:
Last Name:
First Name:

Business Address:

Business:

SSN:
DOB:

b6 -1,3
b7C -1,3

59

Grand Jury Subpoena 0012

United States District Court

SOUTHERN DISTRICT OF NEW YORK

TO:

RECEIVED
SEP 2 ' 2002
FEDEX
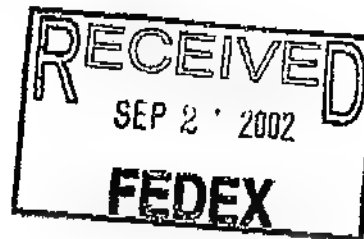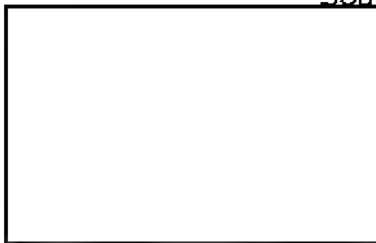
b3 -1
b6 -5
b7C -5
b7D -1
b4 -1

GREETINGS:

WE COMMAND YOU that all and singular business and excuses being laid aside, you appear and attend before the GRAND JURY of the people of the United States for the Southern District of New York, at the United States Courthouse, Foley Square (40 Centre Street), Room 209, in the Borough of Manhattan, City of New York, New York, in the Southern District of New York, at the following date and time:

Appearance Date: [ ]   Appearance Time: [ ]

to testify and give evidence in regard to an alleged violation of:

Title 18, United States Code, Section 1030

and not to depart the Grand Jury without leave thereof, or of the United States Attorney, and that you bring with you and produce at the above time and place the following:

SEE ATTACHED RIDER

N.B.: Personal appearance is not required if the requested documents are delivered or made available on or before the return date to *Special Agent* [ ] Federal Bureau of Investigation, 26

b6 -1
b7C -1

Failure to attend and produce any items hereby demanded will constitute contempt of court and will subject you to civil sanctions and criminal penalties, in addition to other penalties of the Law.

DATED: New York, New York

JAMES B. COMBY
United States Attorney for the
Southern District of New York

b6 -4
b7C -4
b3 -1

James M. Parkman

Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007

Telephone: (212) 637-2277

Full Name:
Last Name:
First Name:

Business Address:

DOB:
SSN:

DL
DL

61

Full Name:
Last Name:
First Name:

e **Business Address:**

b6 -1,3
b7C -1,3

e **Business:**
Mobile:

SSN:
DOB:
Was called by Lamo

May be related to
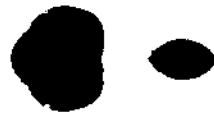
Criminal history

Full Name:
Last Name:
First Name:

Business Address:

SSN:
DOB:

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 8
Page 2 ~ b6 - -1,5,6; b7C - -1,5,6;
Page 3 ~ b6 - -6; b7C - -6;
Page 4 ~ b6 - -5,6; b7C - -5,6;
Page 5 ~ b6 - -1,5,6; b7C - -1,5,6;
Page 6 ~ b6 - -1,5,6; b7C - -1,5,6;
Page 7 ~ b6 - -5,6; b7C - -5,6;
Page 8 ~ b6 - -1,5,6; b7C - -1,5,6;
Page 9 ~ b6 - -5,6; b7C - -5,6;

```
XXXXXXXXXXXXXXXXXXXXXXXXX
X    Deleted Page(s)     X
X    No Duplication Fee  X
X    For this Page       X
XXXXXXXXXXXXXXXXXXXXXXXXX
```

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry   08/11/2013

b7E -3

[redacted] phone number [redacted]
e-mail address [redacted] cc'd writer on e-mail exchanges he had
with [redacted] e mail address [redacted] Also included on
the cc line was [redacted] e-mail address [redacted]   b6 -1,5,6
e-mail address [redacted] e-mail address   b7C -1,5,6
[redacted] and SA [redacted] A response was also
provide by ADRIAN LAMO e-mail address adrian@adrian.org

The e-mail exchanges were electronically attached to this document.

Investigation on 01/16/2013 at Manassas, Virginia, United States (Email)   b6 -1

File # [redacted]   Date drafted 08/11/2013   b7C -1

by [redacted]   b7E -3

FBI(19-cv-1495)-2622

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 5
Page 1 ~ Duplicate;
Page 2 ~ Duplicate;
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X    Deleted Page(s)     X
X    No Duplication Fee  X
X    For this Page       X
XXXXXXXXXXXXXXXXXXXXXXXX
```

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 220
Page 1 ~ b7E - -1;
Page 2 ~ b6 - -5; b7C - -5; b7E - -1;
Page 3 ~ b6 - -5; b7C - -5; b7E - -1;
Page 4 ~ b7E - -1;
Page 5 ~ b6 - -5; b7C - -5; b7E - -1;
Page 6 ~ b7E - -1;
Page 7 ~ b7E - -1;
Page 8 ~ b7E - -1;
Page 9 ~ b7E - -1;
Page 10 ~ b7E - -1;
Page 11 ~ b7E - -1;
Page 12 ~ b7E - -1;
Page 13 ~ b7E - -1;
Page 14 ~ b7E - -1;
Page 15 ~ b7E - -1;
Page 16 ~ b7E - -1;
Page 17 ~ b6 - -5; b7C - -5; b7E - -1;
Page 18 ~ b6 - -5; b7C - -5; b7E - -1;
Page 19 ~ b7E - -1;
Page 20 ~ b7E - -1;
Page 21 ~ b7E - -1;
Page 22 ~ b7E - -1;
Page 23 ~ b7E - -1;
Page 24 ~ b7E - -1;
Page 25 ~ b7E - -1;
Page 26 ~ b7E - -1;
Page 27 ~ b7E - -1;
Page 28 ~ b7E - -1;
Page 29 ~ b7E - -1;
Page 30 ~ b7E - -1;
Page 31 ~ b7E - -1;
Page 32 ~ b7E - -1;
Page 33 ~ b7E - -1;
Page 34 ~ b7E - -1;
Page 35 ~ b7E - -1;
Page 36 ~ b7E - -1;
Page 37 ~ b6 - -5; b7C - -5; b7E - -1;
Page 38 ~ b6 - -5; b7C - -5; b7E - -1;
Page 39 ~ b6 - -5; b7C - -5; b7E - -1;
Page 40 ~ b7E - -1;
Page 41 ~ b7E - -1;
Page 42 ~ b7E - -1;
Page 43 ~ b6 - -5; b7C - -5; b7E - -1;
Page 44 ~ b7E - -1;
Page 45 ~ b6 - -5; b7C - -5; b7E - -1;
Page 46 ~ b7E - -1;
Page 47 ~ b6   5; b7C   5; b7E   1;
Page 48 ~ b6 - -5; b7C - -5; b7E - -1;

```
Page 49 ~ b6 - -5; b7C - -5; b7E - -1;
Page 50 ~ b6 - -5; b7C -  5; b7E - -1;
Page 51 ~ b6 - -5; b7C - -5; b7E - -1;
Page 52 ~ b6 - -5; b7C - -5; b7E - -1;
Page 53 ~ b6 - -5; b7C - -5; b7E - -1;
Page 54 ~ b6 - -5; b7C - -5; b7E - -1;
Page 55 ~ b7E    1;
Page 56 ~ b6 - -5; b7C - -5; b7E - -1;
Page 57 ~ b6 - -5; b7C - -5; b7E - -1;
Page 58 ~ b6 - -5; b7C - -5; b7E - -1;
Page 59 ~ b6 - -5; b7C - -5; b7E - -1;
Page 60 ~ b7E   -1;
Page 61 ~ b7E - -1;
Page 62 ~ b7E - -1;
Page 63 ~ b6 - -5; b7C - -5; b7E - -1;
Page 64 ~ b6 - -5; b7C - -5; b7E - -1;
Page 65 ~ b6 - -5; b7C - -5; b7E - -1;
Page 66 ~ b6 - -5; b7C - -5; b7E - -1;
Page 67 ~ b7E - -1;
Page 68 ~ b7E - -1;
Page 69 ~ b6 - -5; b7C - -5; b7E - -1;
Page 70 ~ b6 - -5; b7C - -5; b7E - -1;
Page 71 ~ b6 - -5; b7C - -5; b7E - -1;
Page 72 ~ b7E - -1;
Page 73 ~ b6 - -5; b7C - -5; b7E - -1;
Page 74 ~ b6 - -5; b7C - -5; b7E - -1;
Page 75 ~ b7E - -1;
Page 76 ~ b6 - -5; b7C - -5; b7E - -1;
Page 77 ~ b7E - -1;
Page 78 ~ b7E - -1;
Page 79 ~ b6 - -5; b7C - -5; b7E - -1;
Page 80 ~ b7E - -1;
Page 81 ~ b6 - -5; b7C - -5; b7E - -1;
Page 82 ~ b7E - -1;
Page 83 ~ b7E - -1;
Page 84 ~ b6 - -5; b7C - -5; b7E - -1;
Page 85 ~ b6 - -5; b7C - -5; b7E - -1;
Page 86 ~ b6 - -5; b7C - -5; b7E - -1;
Page 87 ~ b6 - -5; b7C - -5; b7E - -1;
Page 88 ~ b6 - -5; b7C - -5; b7E - -1;
Page 89 ~ b6 - -5; b7C - -5; b7E - -1;
Page 90 ~ b6 - -5; b7C - -5; b7E - -1;
Page 91 ~ b6 - -5; b7C - -5; b7E - -1;
Page 92 ~ b7E    1;
Page 93 ~ b6 - -5; b7C - -5; b7E - -1;
Page 94 ~ b6 - -5; b7C - -5; b7E - -1;
Page 95 ~ b6 - -5; b7C - -5; b7E - -1;
Page 96 ~ b6 - -5; b7C - -5; b7E - -1;
Page 97 ~ b7E    1;
Page 98 ~ b7E - -1;
Page 99 ~ b6 - -5; b7C - -5; b7E - -1;
Page 100 ~ b7E - -1;
Page 101 ~ b7E -  1;
Page 102 ~ b6 - -5; b7C - -5; b7E - -1;
```

```
Page 103 ~ b6 - -5; b7C - -5; b7E - -1;
Page 104 ~ b6 -  5; b7C    5; b7E    1;
Page 105 ~ b6 - -5; b7C    5; b7E    1;
Page 106 ~ b6 - -5; b7C - -5; b7E - -1;
Page 107 ~ b6 - -5; b7C - -5; b7E - -1;
Page 108 ~ b6 - -5; b7C - -5; b7E - -1;
Page 109 ~ b6 - -5; b7C    5; b7E    1;
Page 110 ~ b6 - -5; b7C    5; b7E    1;
Page 111 ~ b6 - -5; b7C - -5; b7E - -1;
Page 112 ~ b6 - -5; b7C - -5; b7E - -1;
Page 113 ~ b7E - -1;
Page 114 ~ b6 - -5; b7C    5; b7E   -1;
Page 115 ~ b6 - -5; b7C - -5; b7E - -1;
Page 116 ~ b6 - -5; b7C - -5; b7E - -1;
Page 117 ~ b7E - -1;
Page 118 ~ b7E - -1;
Page 119 ~ b6 - -5; b7C - -5; b7E - -1;
Page 120 ~ b6 - -5; b7C - -5; b7E - -1;
Page 121 ~ b6 - -5; b7C - -5; b7E - -1;
Page 122 ~ b7E - -1;
Page 123 ~ b6 - -5; b7C - -5; b7E - -1;
Page 124 ~ b6 - -5; b7C - -5; b7E - -1;
Page 125 ~ b6 - -5; b7C - -5; b7E - -1;
Page 126 ~ b7E - -1;
Page 127 ~ b7E - -1;
Page 128 ~ b6 - -5; b7C - -5; b7E - -1;
Page 129 ~ b6 - -5; b7C - -5; b7E - -1;
Page 130 ~ b7E - -1;
Page 131 ~ b6 - -5; b7C - -5; b7E - -1;
Page 132 ~ b7E - -1;
Page 133 ~ b6 - -5; b7C - -5; b7E - -1;
Page 134 ~ b7E - -1;
Page 135 ~ b7E - -1;
Page 136 ~ b6 - -5; b7C - -5; b7E - -1;
Page 137 ~ b7E - -1;
Page 138 ~ b6 - -5; b7C - -5; b7E - -1;
Page 139 ~ b6 - -5; b7C - -5; b7E - -1;
Page 140 ~ b7E - -1;
Page 141 ~ b7E - -1;
Page 142 ~ b6 - -5; b7C - -5; b7E - -1;
Page 143 ~ b6 - -5; b7C - -5; b7E - -1;
Page 144 ~ b6 - -5; b7C - -5; b7E - -1;
Page 145 ~ b7E - -1;
Page 146 ~ b6 - -5; b7C    5; b7E   -1;
Page 147 ~ b6 - -5; b7C - -5; b7E - -1;
Page 148 ~ b6 - -5; b7C - -5; b7E - -1;
Page 149 ~ b6 - -5; b7C - -5; b7E - -1;
Page 150 ~ b7E - -1;
Page 151 ~ b6 - -5; b7C    5; b7E    1;
Page 152 ~ b6 - -5; b7C - -5; b7E - -1;
Page 153 ~ b6 - -5; b7C - -5; b7E - -1;
Page 154 ~ b6    5; b7C    5; b7E    1;
Page 155 ~ b7E -  1;
Page 156 ~ b6 - -5; b7C - -5; b7E - -1;
```

```
Page 157 ~ b6 - -5; b7C - -5; b7E - -1;
Page 158 ~ b6 -  5; b7C    5; b7E    1;
Page 159 ~ b6 - -5; b7C    5; b7E    1;
Page 160 ~ b7E - -1;
Page 161 ~ b6 - -5; b7C - -5; b7E - -1;
Page 162 ~ b6 - -5; b7C - -5; b7E - -1;
Page 163 ~ b6 - -5; b7C    5; b7E    1;
Page 164 ~ b6 - -5; b7C    5; b7E    1;
Page 165 ~ b7E - -1;
Page 166 ~ b6 - -5; b7C - -5; b7E - -1;
Page 167 ~ b6 - -5; b7C    5; b7E    1;
Page 168 ~ b7E - -1;
Page 169 ~ b6 - -5; b7C - -5; b7E - -1;
Page 170 ~ b6 - -5; b7C - -5; b7E - -1;
Page 171 ~ b6 - -5; b7C - -5; b7E - -1;
Page 172 ~ b6 - -5; b7C - -5; b7E - -1;
Page 173 ~ b7E - -1;
Page 174 ~ b6 - -5; b7C - -5; b7E - -1;
Page 175 ~ b6 - -5; b7C - -5; b7E - -1;
Page 176 ~ b7E - -1;
Page 177 ~ b6 - -5; b7C - -5; b7E - -1;
Page 178 ~ b6 - -5; b7C - -5; b7E - -1;
Page 179 ~ b6 - -5; b7C - -5; b7E - -1;
Page 180 ~ b7E - -1;
Page 181 ~ b6 - -5; b7C - -5; b7E - -1;
Page 182 ~ b6 - -5; b7C - -5; b7E - -1;
Page 183 ~ b6 - -5; b7C - -5; b7E - -1;
Page 184 ~ b6 - -5; b7C - -5; b7E - -1;
Page 185 ~ b6 - -5; b7C - -5; b7E - -1;
Page 186 ~ b6 - -5; b7C - -5; b7E - -1;
Page 187 ~ b6 - -5; b7C - -5; b7E - -1;
Page 188 ~ b6 - -5; b7C - -5; b7E - -1;
Page 189 ~ b6 - -5; b7C - -5; b7E - -1;
Page 190 ~ b7E - -1;
Page 191 ~ b7E - -1;
Page 192 ~ b6 - -5; b7C - -5; b7E - -1;
Page 193 ~ b6 - -5; b7C - -5; b7E - -1;
Page 194 ~ b6 - -5; b7C - -5; b7E - -1;
Page 195 ~ b6 - -5; b7C - -5; b7E - -1;
Page 196 ~ b6 - -5; b7C - -5; b7E - -1;
Page 197 ~ b7E - -1;
Page 198 ~ b7E - -1;
Page 199 ~ b6 - -5; b7C - -5; b7E - -1;
Page 200 ~ b6 - -5; b7C   -5; b7E   -1;
Page 201 ~ b6 - -5; b7C - -5; b7E - -1;
Page 202 ~ b6 - -5; b7C - -5; b7E - -1;
Page 203 ~ b6 - -5; b7C - -5; b7E - -1;
Page 204 ~ b7E - -1;
Page 205 ~ b6 - -5; b7C    5; b7E    1;
Page 206 ~ b6 - -5; b7C - -5; b7E - -1;
Page 207 ~ b6 - -5; b7C - -5; b7E - -1;
Page 208 ~ b6 - -5; b7C    5; b7E    1;
Page 209 ~ b7E -  1;
Page 210 ~ b7E - -1;
```

```
Page 211 ~ b6 - -5; b7C - -5; b7E - -1;
Page 212 ~ b6 -  5; b7C - -5; b7E - -1;
Page 213 ~ b6 - -5; b7C - -5; b7E - -1;
Page 214 ~ b7E - -1;
Page 215 ~ b6 - -5; b7C - -5; b7E - -1;
Page 216 ~ b6 - -5; b7C - -5; b7E - -1;
Page 217 ~ b6 - -5; b7C - -5; b7E - -1;
Page 218 ~ b6 - -5; b7C - -5; b7E - -1;
Page 219 ~ b6 - -5; b7C - -5; b7E - -1;
Page 220 ~ b7E - -1;
```

```
FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-cv-1495

Total Deleted Page(s) = 46
Page 6 ~ b6 - -6; b7C - -6;
Page 7 ~ b3 - -5; b6 - -3,6; b7C    3,6;
Page 8 ~ b3 - -5; b6 - -3,6; b7C - -3,6;
Page 10 ~ b6 - -3; b7C - -3;
Page 11 ~ b6 - -3; b7C - -3;
Page 12 ~ b6 - -3; b7C - -3; b7E   -1;
Page 13 ~ b6 - -3; b7C - -3; b7E - -1;
Page 14 ~ b6 - -3; b7C - -3; b7E - -1;
Page 15 ~ b6 - -3; b7C - -3; b7E - -1;
Page 18 ~ b6 - -5; b7C - -5;
Page 19 ~ b6 - -5; b7C - -5;
Page 20 ~ b6 - -5; b7C - -5;
Page 21 ~ b6 - -5; b7C - -5;
Page 22 ~ b6 - -5; b7C - -5;
Page 23 ~ b6 - -5; b7C - -5;
Page 25 ~ b6 - -6; b7C - -6;
Page 26 ~ b6 - -6; b7C - -6;
Page 27 ~ b6 - -3,5; b7C - -3,5; b7E - -1;
Page 28 ~ b6 - -3,5; b7C - -3,5; b7E - -1;
Page 29 ~ b6 - -3; b7C - -3; b7E - -1;
Page 32 ~ b6 - -3; b7C - -3; b7E - -1;
Page 33 ~ b6 - -3; b7C - -3; b7E - -1;
Page 34 ~ b6 - -3; b7C - -3; b7E - -1;
Page 35 ~ b6 - -5; b7C - -5;
Page 36 ~ b6 - -6; b7C - -6;
Page 37 ~ b6 - -5; b7C - -5;
Page 38 ~ b6 - -5; b7C - -5;
Page 39 ~ b6 - -5; b7C - -5;
Page 40 ~ b6 - -5; b7C - -5;
Page 41 ~ b6 - -5; b7C - -5;
Page 42 ~ b6 - -5; b7C - -5;
Page 43 ~ b6 - -5; b7C - -5;
Page 44 ~ b6 - -6; b7C - -6;
Page 45 ~ b6 - -6; b7C - -6;
Page 47 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 48 ~ b6 - -3,6; b7C - -3,6; b7E - -1;
Page 49 ~ b6 - -3; b7C - -3; b7E - -1;
Page 50 ~ b6 - -3; b7C - -3; b7E    -1;
Page 68 ~ b6 - -1,5; b7C - -1,5;
Page 74 ~ b6 - -5; b7C - -5;
Page 75 ~ b6 - -5; b7C - -5;
Page 79 ~ b6 - -5; b7C - -5; b7E    1;
Page 80 ~ b6 - -5; b7C - -5;
Page 82 ~ b6 - -5; b7C - -5;
Page 83 ~ b6 - -5; b7C - -5;
Page 84 ~ b6 - -5; b7C - -5;

                    XXXXXXXXXXXXXXXXXXXXXXXXX
```

```
X      Deleted Page(s)      X
X      No Duplication Fee X
X      For this Page        X
XXXXXXXXXXXXXXXXXXXXXXXX
```

No

Case ID:

! NY	INTERVIEW NOTES OF	!
! NY	INTERVIEW NOTES OF	!
! NY	DOCUMENTS PROVIDED BY _____ DURING INTERVIEW ON 9/24/2003	!
! NY	INTERVIEW NOTES OF _____ ON 9/9/2003;	!
! NY	INTERVIEW NOTES OF _____ ON 9/9/2003; SEE	!
! NY	INTERVIEW NOTES OF _____ SSN	!
! NY	INTERVIEW NOTES OF	!
! NY	ORGINAL NOTES OF	!
! NY	INTERVIEW NOTES OF _____ ON 10/6/03; SEE	!
! NY	INTERVIEW NOTES OF	!
! NY	E-MAIL B/T SA	!
! NY	INTERVIEW NOTES OF	!
! NY	INTERVIEW NOTES OF 1) NOTES – _____ 2) BUSINESS CARD –	!
! NY	COPIES OF DL & SS CARD _____ 10-13-03; RESPONSE TO QUESTIONS 10-14-03;	!
! NY	COPIES OF _____ BIRTH CERTIFICATE & _____ STATEMENT ABOUT ANOTHER FAMILY MEMBER – RESPONSIBLE??; SEE	!
! NY	INTERVIEW NOTES OF	!
! NY	INTERVIEW NOTES	!

b3 -2
b6 -2,3,5,6
b7C -2,3,5,6
b7E -3

b3 -2
b6 -5,6
b7C -6,6
b7E -3

— See next Volume —

FD-340a (Rev 11-12-89)

(Title)

(File No

1A Suppl.

Item	Date Filed	To be returned			Disposition	
		Yes	No			
	2/13/03		X		*all serial*	

FD-340 (Rev 4-11-0)

File Number _____

Field Office Acquiring Evidence _JN (Jackson)_

Serial # of Originating Document _____

Date Received _12-3-2003_

From _____

(Interviewee)

(Address)

(City and State)

b3 -2
b6 -1,6-
b7C -1,6
b7E -3

By _SA_ _____

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Reference: _FD-302_

(Communication, Enclosing Material)

Description: ☑ Original notes re interview of

b6 -6
b7C -6

FD-340 (Rev. 8-7-97)

Universal Case File Number

Field Office Acquiring Evidence ___WFO___

Serial # of Originating Document ___

Date Received ___09/23/2003___

b3 -2
b6 -1
b7C -1
b7E -3

From ___
(Name of Contributor)

___
(Address of Contributor)

___
(City and State)

By ___SA___
(Name of Special Agent)

To Be Returned ☐ Yes ☑ No
Receipt Given ☐ Yes ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☑ No

Title: ADRIAN LAMO;
NEW YORK TIMES - VICTIM;
COMPUTER INTRUSION;
OO: NY

Reference: ___
(Communication Enclosing Material)

Description: ☑ Original notes re interview of

b6 -3
b7C -3

9/23/03
6:20pm

ADD: ✓

SSN: ✓

FD-340 (Rev. 8-7-97)

Universal Case File Number

Field Office Acquiring Evidence _WF_

Serial # of Originating Document _____

Date Received _9/24/2003_

From _____

(Name of Contributor)

(Address of Contributor)

(State)

b3 -2
b6 -1,6-
b7C -1,6
b7E -3

By _SA_ _____

(Name of Special Agent)

To Be Returned ☐ Yes ☑ No
Receipt Given ☐ Yes ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☐ No

Title: _ADRIAN LAMO;_
NEW YORK TIMES- VICTIM;
COMPUTER INTRUSION;
_OO: NY_

Reference: _____

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

b6 -6
b7C -6

DOCUMENTS PROVIDED BY _____ _DURING INTERVIEW_

_ON 9/24/2003_

FD-340 (Rev. 8-7-97)

Universal Case File Number _____

Field Office Acquiring Evidence _____ *FH - HRA*

Serial # of Originating Document _____

Date Received _____

From _____
<div align="center">(Name of Contributor)</div>

_____
<div align="center">(Address of Contributor)</div>

E_____

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
<div align="center">☐ Yes ☒ No</div>

Title: *ADRIAN LAMO*
NEW YORK TIMES — VICTIM
ComPUTER INTRUSION

Reference: _____
<div align="center">(Communication Enclosing Material)</div>

Description: ☒ Original notes re interview of

_____

b6 -6
b7C -6

ON 9/9/2003

FBI(19-cv-1495)-2552

work seasonally
Dec. – April

FD-340 (Rev. 8-7-97)

Universal Case File Number _____

Field Office Acquiring Evidence _____ *AH - HRA* _____

Serial # of Originating Document _____ [   ] _____

Date Received _____ b3 -2
                                                            b6 -1
From _____ b7C -1
                  (Name of Contributor)   b7E -3

_____
                  (Address of Contributor)

E [   ] gent)

To Be Returned ☐ Yes ☒ No
Receipt Given   ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes ☒ No

Title: *ADRIAN LAMO*
       NEW YORK TIMES - VICTIM
       COMPUTER INTRUSION

Reference: _____
                  (Communication Enclosing Material)

_____

Description: ☒ Original notes re interview of
[   ] *ON 9/9/2003*   b6 -6
                                                     b7C -6

_____

_____

_____

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence Washington FO - NVRA

Serial # of Originating Document _____

Date Received 9/30/2003

                                             b3 -2

From _____   b6 -1

                           b7C -1

(Name of Contributor)   b7E -3

_____

(Address of Contributor)

_____

(City and State)

By SA _____

To Be Returned ☐ Yes   ☒ No

Receipt Given ☐ Yes   ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

        ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)

        ☐ Yes   ☒ No

Title: ADRIAN LAMO;
New York Times - Victim;
Computer Intrusion;
OO: NY

Reference: _____

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

_____   b6 -6

_____   b7C -6

FBI(19-cv-1495)-2574

FD-340b (Rev. 2-5-93)

Universal Case File Number

Field Office Acquiring Evidence _WFO_

Serial # of Originating Document

Date Received _9/25/2008_

From

(or)

(or Contributor)

By

(Name of Special Agent)

b3 -2
b6 -1,2.
b7C -1,2
b7E -3

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

☐ Yes ☑ No

Title:

Reference: _FO-302_

(Communication Enclosing Material)

Description: ☑ Original notes re interview of

b6 -2
b7C -2

No ask./permission _Adrian Lamo_ -

[redacted]

never Been Subscriber, never if possible
but Knowledge never given accent by
anyone. Met one line 5 or 6 years
ago. gone [redacted]

[redacted]

b6 -2,6
b7C -2,6

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ WF ___

Serial # of Originating Document _____

Date Received 09/25/03 _____

From _____ b3 -2
         (Name of Contributor)   b6 -1
                                                            b7C -1
_____ b7E -3
         (Address of Contributor)

_____
         (City and State)

By ___ SA _____

To Be Returned   ☐ Yes   ☐ No
Receipt Given   ☐ Yes   ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                  ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)
                  ☐ Yes   ☒ No

Title:

Reference: _____
              (Communication Enclosing Material)

Description: ☒ Original notes re interviews of

                                                            b6 -2,6
                                                            b7C -2,6

best of knowledge no
lexus

met Lamo while

Lamo was
nice, well kept.
phone & email contact when

always had
not new stuff, same things

always inked that

had aol and dial-in Amer. Univ. & could [b6 -2,6] [b7C -2,6]
click on the icon for AU and

[redacted]

Reclusive, distrustful, studdering but

[redacted]

Lamo called [redacted] [b6 -2,6] [b7C -2,6]

but Lamo doesn't have the #

[redacted]

Lamo didn't/wouldn't tell him who else he stayed with.

[redacted]

[redacted] Lamo had wireless access while [redacted]

97 worked for AOL as a - moderator OutProud - became
"planetOut" "pnomagus" was lamo's screen [b6 -2,5,6] [b7C -2,5,6]
name there but talked to D w/ adrian
.. "sneakylittlefuck" was another "magus2600" ...

[redacted]

adrian's cell
415-5D5-HACK

[redacted] now in Sacramento.

In mid 90's he lived in Arlington, Va. Middle school in Arlington. HS in San Fran. public school.

Lamo said he was being hired by co's to provide comp. security. But wouldn't say anything about it.

Hacking ~~has~~ was his hobby. Wanted to be the hero by exposing vulnerability. He is anti-big company, just made comment about big co's. Never met any friend or associates ~~Anti-big company~~.
He was an out cast

Lamo mentioned hacking WorldCom & AOL. NY Times he hacked and got personal info

AIM - ADRIAN - moderator on OUTPROUD -
Sponsored by AOL.
PNOMA PNO_MAGUS another screen name.
1/2 dozen or [illegible]. Sneaky little fuck.
MAGUS 2600.

[redacted]   b6 -5
                                                                                     b7C -5

[redacted]   (415) 508 HACK adrian cell phone

Adrian lived Mid 90's w/ parents. Arlington.
don't know financial Possibly parents.
told him security consultant in S.F.

Sent links to security focus. Com — news article
thought. Adrian felt good about exposing Vulnerabilities

anti-big company - made comments [redacted]
[redacted]   last contact

[redacted]   b6 -2,6
                                                                                     b7C -2,6

Enemies Large companies Govt.

Lexus Nexus [redacted]   [redacted]

[redacted]   Looking too many secrets.

— A.C. liais with

— approx [ ] was on interview — News media
smelled,
would send articles and web links. Attended

AOL (ISP) Has dial up =.

Sociable become
at first reclusive, distrustful, stutters,. poor hygiene. dishreveled

No friends or acquaintances.

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence _UFO_

Serial # of Originating Document _____

Date Received _10-6-03_

From _____
(Name of Contributor)

b3 -2
b6 -1
b7C -1
b7E -3

_____
(Address of Contributor)

By _SA_ _____

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: ADRIAN LAMO
New York Times—VICTIM
Computer Intrusion

Reference: _____
(Communication Enclosing Material)

Description: ☑ Original notes re interview of _____

b6 -6
b7C -6

_on 10-6-03_

→ adrian looked us [redacted]

→ [redacted]

— lamo → <u>withdrawn</u>, unkempt
    only spoke if spoken to, (quiet)

→ [redacted]

→ lamo ' [redacted] said

→ Media knowledge of attacks.

→ knew [redacted] got money [redacted]
[redacted] him/him to fix hack.

[large redacted box]

[large redacted box]

FD-340b (Rev. 2-5-93)

Universal Case File Number

Field Office Acquiring Evidence _WFO_

Serial # of Originating Document

b3 -2
b6 -1,6
b7C -1,6
b7E -3

Date Received _9/25/2003_

From

(Address of Contributor)

(City and State)

By

(Name of Special Agent)

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant

to Rule 6 (e), Federal Rules of Criminal Procedure

☐ Yes ☑ No

Title:

Reference: _FD-302_

(Communication Enclosing Material)

Description: ☑ Original notes re interview of

b6 -6
b7C -6

Met Sor 6 times.
Lam was meeting

b6 -5,6
b7C -5,6

did corporate intelligence in S.F. also read
about in papers. ADrian odd (eccentric /egotistical.
Showed Stan gun, torch, microsoft. Felt
Lam - rudimentary - basic skills ☆ Knew through

Met as well. Last talked on phone 6 months
ago. Lamo called him. no ask tech advice.
had contact with.

May
Kinkos - primary internet access.
Aim Adrian @   /S.F.

b6 -5,6
b7C -5,6

Security focus - daily .

Lamo -   talked about him.

Lamo never talked about

FBI(19-cv-1495)-2590

ethics — breaking into company & disclose it to them

may ego / vs. good will — no index stace.

goals — Boork — Jut.

cell phone — 415 # (Chargeal (didnt keep)
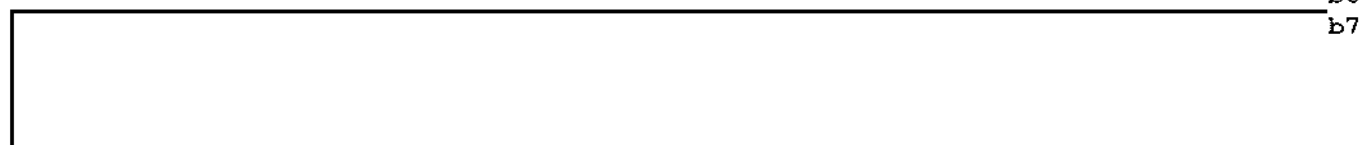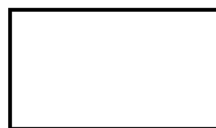
no idea why used modem to contact company
other than ~ vendors dont fix unless made
public.

Laptops (1) Fujitsu lifebook 12.1" screen. gray.
(2000 or 01)

exits to look up [ ] name — read articles:
Si.
illog (illog k) Aim name.

Mark ABENE → Jonathan Quinttu — "Masters of Deception".
"Fiber Optic "

Fujisu lifestyle 12.1" monitor broken
hinges, gray

assumed parents gave him $

Jon Quinter "Masters of disception" the
gang who ruled cyber space.
Character "fiber optic" is Mark Abene

met 5-6x, talked on the phone.

[redacted] Lamo was visiting [redacted] met him

them. The two knew each other [redacted]

Lamo said he had done corp. intel work in San Fran.

Paranoid around new people Egotistical.

AIM - adrian
may have worked for AOL

P.A & San Fran.

walks - rides bus

FD-340 (Rev. 8-7-97)

Universal Case File Number

Field Office Acquiring Evidence _HN_

Serial # of Originating Document

Date Received _9/9/2003_

From

(Name of Contributor)

(Address of Contributor)

(City and State)

b3 -2
b6 -1,5
b7C -1,5
b7E -3.

By _SA_

(Name of Special Agent)

To Be Returned ☐ Yes ☒ No
Receipt Given ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No

Title:
Adrian Lamo;
New York Times - Victim;
Computer Intrusion;
OO: NY

Reference: _FD-302 dated 10/8/2003_
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

e-mail b/f

b6 -1
b7C -1

FD-340 (Rev. 3-8-01)

Universal Case File Number _____

Field Office Acquiring Evidence ___ PX _____

Serial # of Originating Document _____

Date Received ___ 10-3-03 _____

From _____
                                                        b3 -2
                                                        b6 -1
                                                        b7C -1
              (Name of Contributor)   b7E -3

_____
              (Address of Contributor)

_____
              (City and State)

By __SA__ _____

To Be Returned ☐ Yes   ☒ No

Receipt Given   ☐ Yes   ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

                ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)

                ☐ Yes   ☐ No

Title:

Reference: _____
              (Communication Enclosing Material)

Description: ☒ Original notes re interview of
                                                        b6 -5
_____   b7C -5

P/C [redacted]

aug 2000

cox cable modem

[redacted] address

s/l up for [redacted]
w/ ss# + previous employmt.
cox was involved w/ excite@home
& homepage

[redacted] didn't recognize

Security Focus.com

[redacted]

((1))

1) GJ subpoena
2) previous address in
   time frame
   employment there

info

SS#

DOB

Santa Monica based ISP /
dynamic IP address

prior employment at

not familiar
  w/ Lexis/Nexus
Never used

several times were hacked into
+ used was on side of tracker
some work w/ FBI to try + track
used them as a node

b6 -5
b7C -5

served Subpoena

b6 -5
b7C -5

FBI(19-cv-1495)-2599

the River ISP   Email + researching

have had ———→   cd provide all ISPs
if time to   all addresses
research

looks somewhat familiar maybe but
definately not w/ that name.

Doesn't go to hacker sites
Doesn't Do online chat

Q re: responding to subpoena ——

FD-340 (Rev 4-11-03)

File Number _____

Field Office Acquiring Evidence _____ BOSTON

Serial # of Originating Document _____

Date Received _____ 10/01/2003

From _____ SELF
(Name of Contributor/Interviewee)

_____
(Address)

_____
(City and State)

By _____ SA

To Be Returned   ☐ Yes   ☑ No

Receipt Given   ☐ Yes   ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes   ☑ No

Federal Taxpayer Information (FTI)

☐ Yes   ☑ No

Reference. _____ FD 302
(

Description: ☑ Original notes re interview of

1) NOTES

2) BUSINESS CARD

b3 -2
b6 -1
b7C -1
b7E -3

b6 -5
b7C -5

FBI(19-cv-1495)-2601

10/1/03

[REDACTED]   · MET IN PASSING ·   b6 -5
                                    b7C -5

[REDACTED]   — MET   [REDACTED]

[REDACTED]

[REDACTED]   — INTERVIEW SECURITY TOPICS

[REDACTED]
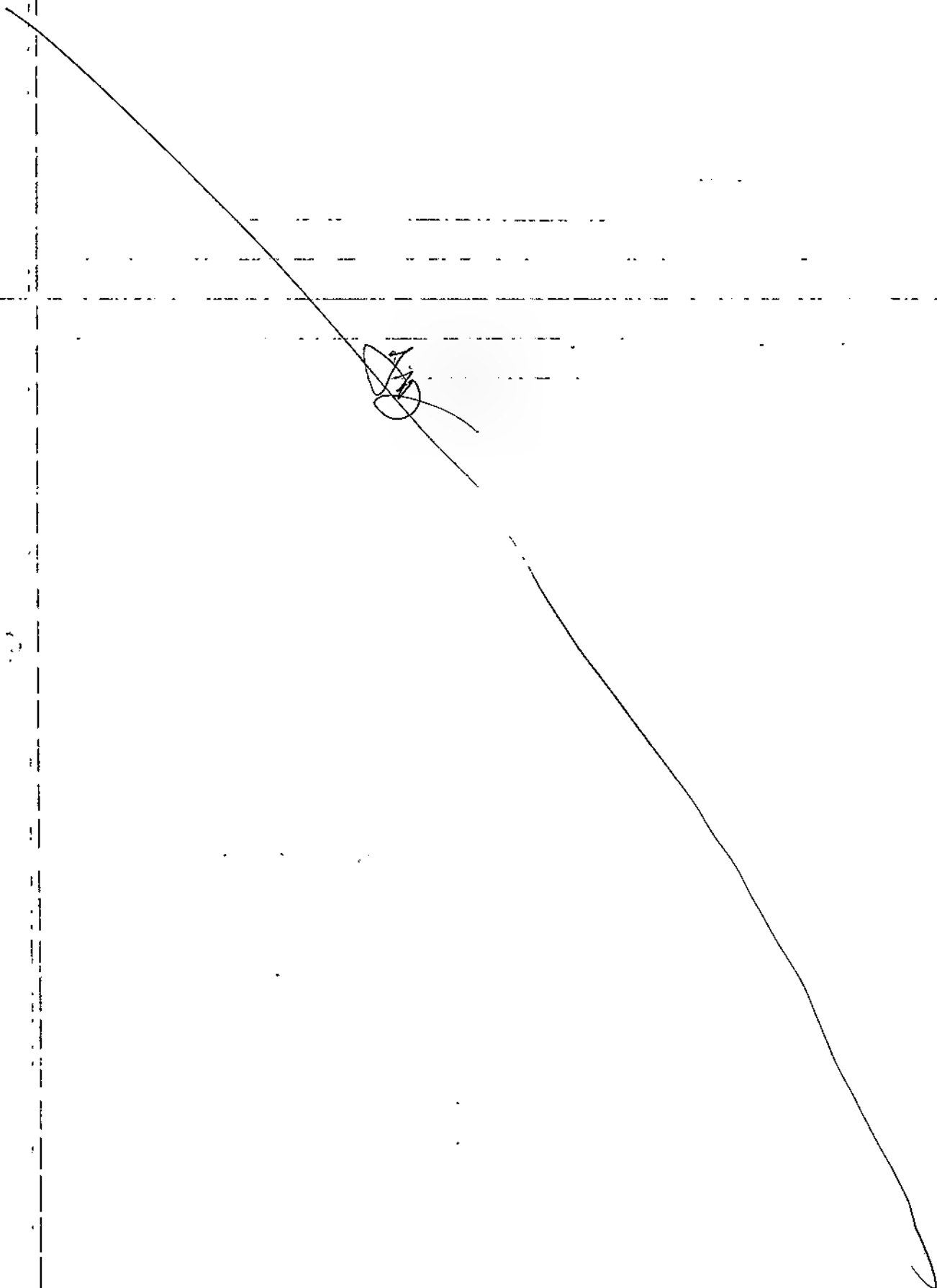
Universal Case File Number _____

Field Office Acquiring Evidence _____ SC _____

Serial # of Originating Document _____

Date Received _____ 10 | 13 + 14 | 2003 _____

From _____

(Name of Contributor)

b3 -2
b6 -1,5
b7C -1,5
b7E -3

(Address of Contributor)

(City and State)

By _____

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title: ADRIAN LAMO

Reference: _____

(Communication Enclosing Material)

Description: ☐ Original notes re interview of _____

b6 -5
b7C -5

COPIES OF DL + SS CARD   10-13-03

Respone TO questions   10-14-03

FD-340 (7-19-00)

Universal Case File Number _____

Field Office Acquiring Evidence _____ SC _____

Serial # of Originating Document _____

Date Received _____ 10/13/2003 _____

From _____

(Name of Contributor)

_____

(Address of Contributor)

_____

(City and State)

b3 -2
b6 -1,5
b7C -1,5
b7E -3

By _____

To Be Returned   ☐ Yes   ☒ No

Receipt Given   ☐   ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

     ☐ Yes   ☒ No

Federal Taxpayer Information (FTI)

     ☐ Yes   ☒ No

Title: ADRIAN LAMO

Reference: _____

(Communication Enclosing Material)

_____

Description: ☐   Original notes re interview of

copies of _____   BIRTH certificate.

+ _____   About Another

Sony number — responsible ??

b6 -5
b7C -5

FBI(19-cv-1495)-2609

FD-340 (Rev 3-8-01)

Universal Case File Number

Field Office Acquiring Evidence   *15C*

Serial # of Originating Document

Date Received   *10 - 10 - 03*

From *SA*   b6 -1
                                       b7C -1
          (Name of Contributor)   b3 -2
                                       b7E -3
    SA

          (Address of Contributor)

          (City and State)

By *SA*

To Be Returned   ☐ Yes   ☐ No

Receipt Given   ☐ Yes   ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

          ☐ Yes   ☐ No

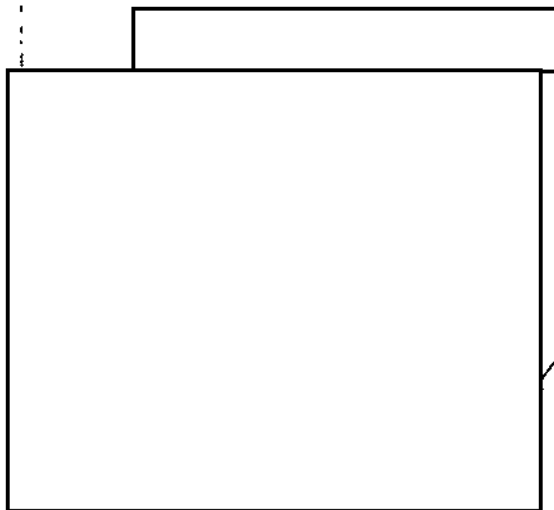Federal Taxpayer Information (FTI)

          ☐ Yes   ☐ No

Title:

Reference _____

          (Communication Enclosing Material)

_____

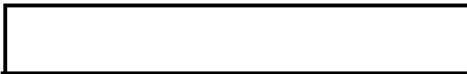**Description:**   ☑ Original notes re interview of   b6 -6
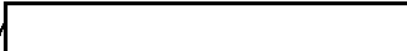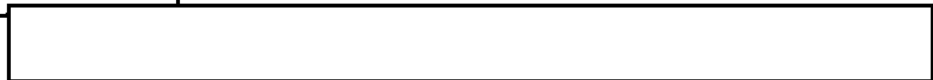   b7C -6
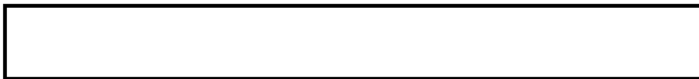
Interview

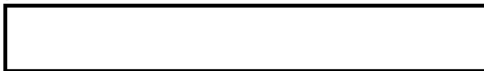when met

outside of San Fran

Adrian Alfonso Lamo

St number)

Working at

Adrian - knows IBM

met

been there several times

Adrian- born in Arlington, VA

Lowell High School- Lamo went there
gifted kid
Wrote own version of DOS
taught himself Assembler

contacted [REDACTED] via email and told
   him about EXCITE / CNET
Saw him [REDACTED]
   — Working There [REDACTED]

Contacts [REDACTED]
   "   via IM

adrian @ adrian.org   >
darklord @ darkthrone.net

[REDACTED]

AOL magos
archane
bittergeek
60
Linetrace
Loanhackor
Lord of flies
Lord of files
Lord of rings
matrix
Security team
subversive
tom ammjino
true faith

AOL Screennames

[REDACTED] contacted Adrian
41S- SOS- HACK
         ↳ adrian's cell phone

[REDACTED] contacted via email

Screenname

ISP = SW bell
Ethernet @ work

Not a hacker

Doesn't frequent chat rooms

at times tempermental ~ normal guy
Never called here

At Worked for some company on market st. in SF
gets on web at Kinko's + wireless
supporting himself
Never shared financial details

hacking tools - web browser

Non-committed person

[redacted]

didn't take drugs when he knew him

One laptop

Toshiba laptop, win 98, 2-3 yrs old

[redacted]

I said he didn't like [redacted]

No enemies

Sent one screenshot once— does't remember

[redacted] have online access now

[redacted]

screen name

[redacted]

self taught, [redacted]

lives m [redacted]

White male

10-6-0[?]

tech

C.H.

b6 -6
b7C -6

APPLE

ISP
SWB

1996   ADRIAN ALPHONSO LAMO   POB
ARLINGTON, VA

LAMO

SAN FRANCISCO

b6 -5,6
b7C -5,6

IBM DOS/WIN   LAMO

VA

ADV. H.S. LOWELL   TESTED OUT 1 YR EARLY
L WRITTEN OWN VERSION DOS
L LEARNED ASSEMBLER

3 YRS. SF LYRIC → LAB
messenger   adrian@adrian.org
            dark/ord@dark throne.net
loneharger   aol magus
lord of flies   arcane   subversive
lord of files   bittergeek   tomamriano
lord of rings   go   truefaith
matrix   ninetrace
security team

FBI(19-cv-1495)-2618

②

WIRELESS - AP   10/6

KINKO'S

[redacted]   (CONTACTED) H??   b6 -6
                                              b7C -6
        4/5   SOS (HACK

④ [redacted]

Lyric in ????

6
7
8
CAMO

⑧ [redacted] PERSON   PH?? [redacted]   b6 -6
      [redacted]   b7C -6

42 TOSHIBA   WIN 98
43 [redacted]

47 LYRIC
    CAMO WENT AFTER [redacted]
54 [redacted]

W/M   b6 -5
                                                b7C -5
WIN/?

FD-340 (Rev. 8-7-97)

Universal Case File Number _____

Field Office Acquiring Evidence _____ M W _____

Serial # of Originating Document _____

Date Received _____ 10 /10/ 2 003 _____

From _____
(Name of Contributor)

b3 -2
b6 -1,5
b7C -1,5
b7E -3

_____
(Address of Contributor)

_____
(City and State)

By _____ S A _____
(Name of Special Agent)

To Be Returned ☐ Yes ☒ No
Receipt Given   ☐ Yes ☒ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☒ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☑ Original notes re interview of _____

b6 -5
b7C -5

_____

_____

_____

FBI(19-cv-1495)-2620

No

- No phone books

- No
- Possibly

- Well versed